

Министерство образования и науки Российской Федерации  
ФГБОУ ВО «Уральский государственный педагогический университет»  
Институт математики, информатики и информационных технологий  
Кафедра высшей математики

**Использование системы компьютерной алгебры GАР для исследования  
конечномерных алгебр**

Выпускная квалификационная работа

Квалификационная работа  
допущена к защите  
Зав. кафедрой

\_\_\_\_\_  
дата                      подпись

Исполнитель:  
Леванидзе Анна Сергеевна,  
обучающаяся Б-42 группы

\_\_\_\_\_  
подпись

Руководитель ОПОП:

\_\_\_\_\_  
подпись

Научный руководитель:  
Коробков С.С.,  
к.ф.-м.н., доцент

\_\_\_\_\_  
подпись

Екатеринбург 2017

## Оглавление

<b>Введение .....</b>	<b>3</b>
<b>ГЛАВА I. Теоретические основы .....</b>	<b>5</b>
§ 1. Основные алгебраические структуры .....	5
§ 2. Алгебры над полем .....	14
§ 3. Элементы теории решеток .....	22
<b>ГЛАВА II. Система компьютерной алгебры GAP .....</b>	<b>26</b>
§ 1. Общее описание .....	26
§ 2. Язык программирования GAP .....	28
§ 3. Основные команды, используемые в работе .....	29
§ 4. Простейшие программы вычислений в матричной алгебре .....	30
<b>ГЛАВА III. Исследования конечномерных алгебр .....</b>	<b>31</b>
§ 1. Тип решетки .....	31
§ 2. Алгоритм исследования четырехмерных подалгебр .....	31
§ 3. Алгоритм построения диаграммы решетки подалгебры .....	43
<b>Библиографический список.....</b>	<b>53</b>
<b>Приложения .....</b>	<b>54</b>

## Введение

В дипломной работе рассматривается алгебра порядка 3 над полем из двух элементов  $M_3(GF(2))$ , которая содержит  $2^9=512$  элементов. Из ранее полученных результатов известно, что количество подалгебр равняется 2102 [7]. На данный момент классифицированы все подалгебры порожденные одним элементом [8] алгебры  $A$ , а также двухмерные, трехмерные подалгебры [9]. Количество четырехмерных подалгебр равняется 497 [7], но их решетки подалгебр до настоящего времени оставались неизученными.

**Целью** данной дипломной работы является разработка алгоритмов и программ для изучения и классификации с точностью до изоморфизма четырехмерных подалгебр алгебры  $M_3(GF(2))$  и построение диаграмм их решеток подалгебр. Данная цель достигается с помощью системы компьютерной алгебры GAP и решения следующих задач:

1. Разработать алгоритмы для нахождения подалгебр алгебры матриц порядка 16 над полем из двух элементов.
2. На основе разработанных алгоритмов составить программы в компьютерном пакете GAP для нахождения подалгебр, заданных порождающими элементами.
3. Для каждой из найденных подалгебр определить ее тип решетки.
4. Получить типовую классификацию найденных подалгебр.
5. Для каждого типа подалгебр построить диаграммы решеток подалгебр.

**Актуальность** выбора темы: заключается в необходимости создания большой базы примеров конечномерных алгебр с различными алгебраическими свойствами и типами решеток подалгебр. Наличие такой базы позволит осуществлять проверку гипотез и строить контрпримеры при изучении решеточных свойств алгебр.

Работа состоит из трех глав, списка литературы и приложений.

Первая глава содержит теоретические основы исследований. В ней приведены основные алгебраические структуры и их основные свойства. Во вто-

ром параграфе приводятся определение алгебры над полем, подалгебры и изоморфизм алгебр. Кроме того, приводятся примеры, а также рассматриваются основные теоремы. Третий параграф посвящен элементам теории решеток.

Вторая глава посвящена системе компьютерной алгебры GAP. Этот пакет является многофункциональным, простым в изучении, универсальным и что не маловажно – GAP находится в открытом доступе в сети Интернет. Первый параграф посвящен определению GAP и истории его создания, а также описываются этапы установки и системные требования. Также приведено описание справочной системы GAP. Вторым параграфом посвящен языку программирования системы компьютерной алгебры GAP. В нем приводятся примеры ключевых слов, идентификаторов и выражений. Далее представлены основные команды, используемые в практической работе, а также приведены простейшие программы вычислений в матричной алгебре.

Практическая часть представлена в третьей главе. Здесь описывается алгоритм построения подалгебр в алгебре квадратных матриц порядка три над полем из двух элементов. Приводятся алгоритмы для вычисления типов решеток подалгебр. Из найденных ранее подалгебр данной алгебры предыдущими выпускниками направления «Прикладная информатика и математика», выбраны некоторые подалгебры, которые еще не были исследованы и для них приведена классификация с точностью до изоморфизма. Полученные данные описаны и представлены в выпускной квалификационной работе в виде написанных программ и таблиц с результатами, которые располагаются в приложении, а также графически представлены типы решеток.

# ГЛАВА I. Теоретические основы

## §1. Основные алгебраические структуры

### Понятие группы. Примеры групп

**Определение 1.** Множество  $G$  называется группой, если на нём определена бинарная операция  $\circ$ , удовлетворяющая условиям:

- 1)  $(\forall a, b, c \in G)(a \circ (b \circ c) = (a \circ b) \circ c)$  (ассоциативность);
- 2)  $(\exists e \in G)(\forall a \in G)(a \circ e = e \circ a = a)$  (наличие нейтрального элемента);
- 3)  $(\forall a \in G)(\exists a' \in G)(a \circ a' = a' \circ a = e)$  (наличие симметричного элемента).

Замечание 1. Если операция  $\circ$  является умножением, то будем обозначать её  $\cdot$  и опускать точку в тех случаях, когда ясно, что рассматривается произведение (то есть  $a \cdot b \cdot c = abc$ ). Симметричный элемент  $a'$  будем называть обратным, и будем обозначать  $a^{-1}$  (то есть  $a' = a^{-1}$ ). В таких случаях группу  $G$  будем называть мультипликативной. Если операция  $\circ$  является сложением, то группу  $G$  будем называть аддитивной, нейтральный элемент  $e$  будем обозначать  $0$  (то есть  $e = 0$ ), а симметричный элемент  $a'$  обозначать  $-a$  (то есть  $a' = -a$ ).

Примеры групп.

а) Аддитивная

1.  $G = (Z, +)$  – группа целых чисел.
2.  $G = (Q, +)$  – группа рациональных чисел.
3.  $G = (V, +)$ , где  $V$  – множество геометрических векторов в трехмерном евклидовом пространстве.
4.  $G = (\bar{Z}, +)$ , где  $\bar{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$  – классы целых чисел по модулю 7. Сложение определяется по следующей формуле  $\bar{a} + \bar{b} = \overline{a + b}$ .

Таблица 1. Таблица сложения

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

## b) Мультипликативная

1.  $G = (R \setminus \{0\}, \cdot)$  – группа действительных чисел.
2.  $G = (C \setminus \{0\}, \cdot)$  – группа комплексных чисел.
3.  $G = (M_n(R), \cdot)$  – группа невырожденных матриц порядка  $n$ .
4.  $G = (\bar{Z}, \cdot)$ , где  $\bar{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$  – классы ненулевых целых чисел по

модулю 7. Умножение определяется по следующей формуле  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ .

Таблица 2. Таблица умножения

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

**Основные свойства групп**

Свойство 1. В любой группе  $G$  нейтральный элемент единственен.

Доказательство. Пусть  $e_1, e_2$  – два нейтральных элемента в группе  $G$ , тогда  $e_1 = e_1 \circ e_2 = e_2$ .

Свойство 2. В любой группе  $G$  для каждого элемента из  $G$  существует единственный симметричный элемент.

Доказательство. Пусть  $a'_1$  и  $a'_2$  – симметричные элементы для элемента  $a$  в группе  $G$ . Тогда  $a'_1 = a'_1 \circ e = a'_1 \circ (a \circ a'_2) = (a'_1 \circ a) \circ a'_2 = e \circ a'_2 = a'_2$

Свойство 3. В любой группе  $G$  для элементов  $a$  и  $b$  уравнения  $a \circ x = b$ ,  $y \circ a = b$  имеют единственное решение  $x = a' \circ b$ ,  $y = b \circ a'$ , соответственно.

Доказательство. Докажем, что решение существует.

$$1) a \circ (a' \circ b) = (a \circ a') \circ b = e \circ b = b;$$

$$2) (b \circ a') \circ a = b \circ (a' \circ a) = b \circ e = b.$$

Докажем, что решение единственно.

Пусть  $c \in G$ ,  $a \circ c = b$ , тогда:

$$a' \circ (a \circ c) = a' \circ b,$$

$$(a' \circ a) \circ c = a' \circ b,$$

$$e \circ c = a' \circ b,$$

$$c = a' \circ b.$$

Единственность решения второго уравнения доказывается аналогично.

Свойство 4. Правило сокращения.

$$(\forall a, b, c \in G)(a \circ b = a \circ c \Rightarrow b = c)$$

Доказательство.  $b = e \circ b = (a' \circ a) \circ b = a' \circ (a \circ b) = a' \circ (a \circ c) = (a' \circ a) \circ c = e \circ c = c$ .

## Понятие подгруппы. Примеры подгрупп

**Определение 2.** Подмножество  $S$  группы  $G$  называется подгруппой группы  $G$ , если  $S$  является группой относительно операции  $\circ$ , определенной на множестве  $G$ .

Примеры подгрупп.

1.  $S = (Z, +)$  является подгруппой группы  $G = (Q, +)$ .

2.  $G = (Q \setminus \{0\}, \cdot)$  – группа.  $S = Q^+$  – множество положительных рациональных чисел является подгруппой группы  $G$ .

3.  $G = (M_n(C), +)$  – группа невырожденных матриц порядка  $n$  с комплексными элементами.  $S = M_n(R)$  – множество невырожденных матриц порядка  $n$  с действительными элементами является подгруппой группы  $G$ .

### Признаки подгруппы

**Теорема 1.** *(Первый признак подгруппы) Непустое подмножество  $S$  группы  $(G, \cdot)$  тогда и только тогда является подгруппой в группе  $G$ , когда выполняются следующие условия:*

$$1) (\forall a, b \in S)(ab \in S);$$

$$2) (\forall a \in S)(a^{-1} \in S).$$

Доказательство. Необходимость. Пусть  $S$  – подгруппа группы  $G$ . Докажем, что выполняются условия 1) и 2). Условие 1) выполняется, так как в группе  $S$  и  $G$  одна и та же операция. По свойству 2 групп элемент  $a^{-1}$  – единственен, значит  $a^{-1} \in S$ .

Достаточность. Пусть выполняются условия 1) и 2). Докажем, что  $S$  – подгруппа группы  $G$ . Из условия 1) следует, что операция умножение, определенная на группе  $G$ , определена и в  $S$ .

Умножение ассоциативно в  $S$ , так как оно ассоциативно в группе  $G$ .

Из того, что  $S \neq \emptyset$  следует, что существует хотя бы один элемент  $a \in S$ . Тогда в  $S$  содержится обратный элемент и потому  $a \cdot a^{-1} \in S$  и  $a \cdot a^{-1} = e$  откуда следует  $e \in S$ . Из этого следует, что  $S$  – подгруппа группы  $G$ .

**Теорема 2.** *(Второй признак подгруппы) Пусть  $(G, \cdot)$  – мультипликативная группа и  $S$  – непустое подмножество в группе  $G$ . Подмножество  $S$  тогда и только тогда является подгруппой в группе  $G$ , когда выполняется условие:*

$$(\forall a, b \in S)(ab^{-1} \in S).$$



Доказательство. Необходимость. Пусть  $S$  – подгруппа и  $a, b \in S$ . Тогда  $b^{-1} \in S$ . Значит  $ab^{-1} \in S$ .

Достаточность. Пусть выполняется условие  $(\forall a, b \in S)(ab^{-1} \in S)$ . Докажем что  $S$  – подгруппа группы  $G$ . По условию  $S$  – непустое подмножество. Воспользуемся первым признаком подгруппы. Значит  $(\exists a \in S)$ . По условию  $a \cdot a^{-1} \in S \Rightarrow e \in S$ . Воспользуемся условием к элементам  $e$  и  $a$ . Тогда  $(\forall a \in S)(ea^{-1} = a^{-1} \in S)$ . Значит условие 2) в теореме 1 выполнено. Пусть  $a, b \in S$ . Тогда  $ab^{-1} \in S$ . Значит  $ab = a(b^{-1})^{-1} \in S$ . Таким образом, условие 1) и 2) теоремы 1 выполнены, следовательно  $S$  – подгруппа.

## Основы теории колец

**Определение 3.** Множество  $K$  с двумя алгебраическими операциями  $+$ ,  $\cdot$  будем называть ассоциативным кольцом, если выполняются следующие условия:

- 1)  $(\forall a, b \in K)(a + b = b + a)$ ;
- 2)  $(\forall a, b, c \in K)(a + (b + c)) = ((a + b) + c)$ ;
- 3)  $(\exists 0 \in K)(\forall a \in K)(a + 0 = a)$ ;
- 4)  $(\forall a \in K)(\exists (-a) \in K)(a + (-a) = 0)$ ;
- 5)  $(\forall a, b, c \in K)(a(bc) = (ab)c)$ ;
- 6)  $(\forall a, b, c \in K)((c(a + b) = ca + cb) \wedge ((a + b)c = ac + bc))$ .

Условия 1) – 6) называются аксиомами кольца.

Замечание 2. Если в определение 3 исключить аксиому 5), то получим определение кольца.

Если умножение в кольце  $K$  – коммутативно, то  $K$  называется коммутативным кольцом. Если относительно умножения существует нейтральный элемент в кольце  $K$ , то  $K$  называется кольцом с единицей. Если в кольце  $K$  операция умножения коммутативна, ассоциативна и содержится

единичный элемент, то кольцо  $K$  будем называть кольцом с делением, если в нём для каждого ненулевого элемента существует обратный элемент.

Примеры колец.

Таблица 3. Примеры колец

Кольца	Коммутативное кольцо	Кольцо с единицей	Кольцо с делением
$(\mathbb{Z}_2, +, \cdot)$ – четные целые числа	+	–	–
$(R, +, \cdot)$	+	+	+
$(M_n(R), +, \cdot)$	–	+	+(односторонние)
$(R[x], +, \cdot)$	+	+	–

### Основные свойства колец

Пусть  $(K, +, \cdot)$  – произвольное ассоциативное кольцо.

Свойство 1.  $(K, +)$  – абелева группа;

Свойство 2.  $(K, \cdot)$  – мультипликативная полугруппа;

Свойство 3.  $(\forall a \in R)(0 \cdot a = a \cdot 0 = 0)$ ;

Доказательство.  $0 + 0 = 0 \Rightarrow a(0 + 0) = a \cdot 0 + 0 \cdot a = a \cdot 0 \Rightarrow a \cdot 0 + 0 = a \cdot 0 \Rightarrow a \cdot 0 + a \cdot 0 = a \cdot 0 + 0 \Rightarrow 0 \cdot a = a \cdot 0 = 0$ .

Свойство 4.  $(\forall a, b \in K)(a(-b) = (-a)b = -ab)$ ;

Доказательство.  $0 = a \cdot 0 = a(b - b) = a(b + (-b)) = ab + a(-b) \Rightarrow a(-b) = -ab$ .

Второе равенство доказывается аналогично.

Свойство 5.  $(\forall a, b, c \in K)((a(b - c) = ab - ac) \wedge ((b - c)a = ba - ca))$ .

Доказательство.  $a(b - c) = a(b + (-c)) = ab + (-ac) = ab - ac$ .

Второе равенство доказывается аналогично.

### Подкольца. Признак подкольца

**Определение 4.** Пусть  $(K, +, \cdot)$  – кольцо. Подмножество  $S$  в  $K$  называется подкольцом кольца  $K$ , если  $(S, +, \cdot)$  – кольцо.

Примеры подколец.

1.  $K = (M_n(R), +, \cdot)$  – кольцо невырожденных матриц порядка  $n$  с действительными элементами.  $S$  – множество матриц порядка  $n$ , в которых под главной диагональю располагаются нули является подкольцом кольца  $K$ .

2.  $K = (R[x], +, \cdot)$  – кольцо многочленов.  $S$  – множество многочленов, в которых свободный член равен нулю является подкольцом кольца  $K$ .

**Теорема 3.** (Признак подкольца) *Непустое подмножество  $S$  кольца  $(K, +, \cdot)$  тогда и только тогда является подкольцом в  $K$ , когда выполняются следующие условия:*

$$1) (\forall a, b \in S)((a - b) \in S);$$

$$2) (\forall a, b \in S)(ab \in S).$$

Доказательство. Необходимость. Пусть  $S$  – подкольцо в  $K$ . Тогда  $S$  замкнуто относительно умножения, значит выполнено условие 2) и  $(S, +)$  является подгруппой в  $(K, +)$  и потому по теореме 2 выполняется условие 1).

Достаточность. Пусть выполнено условие 1) и 2). Из выполнимости 1) вытекает, что  $(S, +)$  является подгруппой в группе  $(K, +)$ , это значит, что сложение в  $S$  определено и аксиомы кольца 1) – 4) выполнены. Из выполнимости условия 2) следует, что умножение определено на  $S$  и значит, выполняется условие 5. Таким образом,  $S$  – подкольцо.

### Понятие поля. Примеры полей

**Определение 5.** *Множество  $F$ , содержащее не менее двух элементов называется полем, если на нем определены две бинарные алгебраические операции  $+$ ,  $\cdot$  удовлетворяющие следующим условиям:*

$$1) (\forall a, b, c \in F)(a + (b + c)) = ((a + b) + c);$$

$$2) (\forall a, b \in F)(a + b = b + a);$$

$$3) (\exists 0 \in F)(\forall a \in F)(a + 0 = a);$$

$$4) (\forall a \in F)(\exists (-a) \in F)(a + (-a) = 0);$$

$$5) (\forall a, b, c \in F)(a(bc) = (ab)c);$$

- 6)  $(\forall a, b \in F)(ab = ba)$ ;
- 7)  $(\exists 1 \in F)(\forall a \in F)(1 \cdot a = a)$ ;
- 8)  $(\forall a \in F \setminus \{0\})(\exists a^{-1} \in F \setminus \{0\})(a \cdot a^{-1} = 1)$ ;
- 9)  $(\forall a, b, c \in K)(a(b + c) = ab + ac)$ .

Условия 1) – 9) называются аксиомами поля.

Примеры полей.

1.  $\mathbb{Q}$  – поле рациональных чисел.
2.  $\mathbb{R}$  – поле действительных чисел.
3. Конечные поля – поля Галуа. Самое маленькое поле имеет два элемента, операции сложения и умножения задаются следующими таблицами:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

### Основные свойства полей

Пусть  $(F, +, \cdot)$  – поле.

Свойство 1.  $(F, +)$  – абелева группа;

Свойство 2.  $(F \setminus \{0\}, \cdot)$  – мультипликативная абелева группа;

Свойство 3.  $(F, +, \cdot)$  – коммутативное ассоциативное кольцо с единицей и с делением;

Свойство 4. Нулевой элемент не имеет обратного элемента в любом поле.

Доказательство. Пусть  $b$  – обратный элемент к элементу 0. Тогда  $0 \cdot b = 1$  и по свойству  $0 \cdot b = 0$ . Значит  $1 = 0$ . Тогда по аксиоме 7 поля  $(\forall a \in F)(a \cdot 1 = a = 0)$ . Получили противоречие с определением поля, а именно что в поле не менее двух элементов.

### Понятие подполя. Примеры подполей. Признак подполя

**Определение 6.** Подмножество  $S$  поля  $F$  называется подполем поля  $F$ , если само  $S$  является полем относительно операций  $+, \cdot$  определенных в поле  $F$ .

Примеры подполей.

1.  $Q$  – подполе поля  $R$ .
2.  $Q$  – подполе поля  $C$ .
3.  $R$  – подполе поля  $C$ .

**Теорема 4. (Признак подполя)** Подмножество  $S$ , содержащее не менее двух элементов тогда и только тогда является подполем поля  $F$ , когда выполняются следующие условия:

- 1)  $(\forall a, b \in S)((a - b) \in S)$ ;
- 2)  $(\forall a, b \in S)(ab \in S)$ ;
- 3)  $(\forall a \in S \setminus \{0\})(a^{-1} \in S)$ .

Доказательство. Необходимость. Пусть  $S$  – подполе поля  $F$ . Тогда  $S$  является полем относительно операций  $+$ ,  $\cdot$ , следовательно, условия 1) – 3) выполняются.

Достаточность. Пусть выполнены условия 1) – 3). Из условий 1) и 2) следует, что  $S$  – подкольцо в  $(F, +, \cdot)$ , а значит, выполнены аксиомы поля 1) – 4) и условия ассоциативности и дистрибутивности умножения. Из выполнимости условия 3) следует, существование обратных элементов в  $S$  и существование единичного элемента. Значит, аксиома поля 7) выполнена. Аксиома 6) выполняется, так как умножение коммутативно в поле  $F$ . Таким образом,  $S$  – подполе.

## Векторные пространства, примеры

**Определение 7.** Векторным (линейным) пространством над полем  $P$  называется множество  $V$  с определенной на нем бинарной, алгебраической операцией сложения  $+$  и операцией умножения элементов из  $P$  на элемент из  $V$  со значениями в  $V$ , удовлетворяющее условиям:

- 1)  $(\forall a, b \in V)(a + b = b + a)$ ;
- 2)  $(\forall a, b, c \in V)(a + (b + c) = (a + b) + c)$ ;
- 3)  $(\exists \bar{0} \in V)(\forall a \in V)(a + \bar{0} = a)$ ;
- 4)  $(\forall a \in V)(a + (-a) = \bar{0})$ ;

- 5)  $(\forall a \in V)(\forall \alpha, \beta \in P)(\alpha(\beta a) = (\alpha\beta)a)$ ;
- 6)  $(\forall a, b \in V)(\forall \alpha \in P)(\alpha(a + b) = \alpha a + \alpha b)$ ;
- 7)  $(\forall a \in V)(\forall \alpha, \beta \in P)(\alpha(\beta a) = (\alpha + \beta)a = \alpha a + \beta a)$ ;
- 8)  $(\forall a \in V)(1 \cdot a = a)$ .

Элементы из  $V$  будем называть векторы, а из  $P$  – скаляры.

Примеры векторных пространств.

1.  $V_3$  – линейное пространство векторов пространства;
2.  $V = \mathbb{C}, P = \mathbb{R}$ ;
3.  $V = \mathbb{C}, P = \mathbb{C}$ ;
4.  $V = P[x], P = \mathbb{R}$ .

### Простейшие свойства линейных пространств

Свойство 1.  $(\forall a \in V)(0 \cdot a = 0)$ .

Свойство 2.  $(\forall \alpha \in P)(\alpha \cdot \bar{0} = \bar{0})$ .

Свойство 3.  $(\forall \alpha \in P)(\forall a \in V)(\alpha a = a \Leftrightarrow \alpha = 0 \vee a = \bar{0})$ .

Свойство 4.  $(\forall \alpha \in P)(\forall a \in V)(\alpha(-a) = (-\alpha)a = -\alpha a)$ .

Свойство 5.  $(\forall \alpha \in P)(\forall a, b \in V)(\alpha(a - b) = \alpha a - \alpha b)$ .

Свойство 6.  $(\forall \alpha, \beta \in P)(\forall a \in V)((\alpha - \beta)a = \alpha a - \beta a)$ .

## §2. Алгебры над полем

### Определение алгебры над полем

**Определение 8.** Алгеброй над полем  $P$  называется множество  $A$  с определенными на нём двумя бинарными, алгебраическими операциями сложения  $+$  и операцией умножения элементов из  $P$  на элемент из  $A$ , удовлетворяющее следующим условиям:

- 1)  $(A, +, \cdot)$  – кольцо;
- 2)  $(A, +, \cdot)$  – векторное пространство над  $P$ ;
- 3)  $(\forall \alpha \in P)(\forall a, b \in A)(\alpha(ab) = (\alpha a)b = a(\alpha b))$ .

Если кольцо  $(A, +, \cdot)$  является ассоциативным (коммутативным, с единицей, с делением), то и алгебра  $A$  называется ассоциативной (коммутативной, с единицей, с делением соответственно).

Представим условия 1) – 3) определения 8 в развернутом виде, в результате получим следующее определение:

**Определение 9.** Алгеброй над полем  $P$  называется множество  $A$  с определенными на нём двумя бинарными, алгебраическими операциями сложения  $+$  и операцией умножения элементов из  $P$  на элемент из  $A$ , удовлетворяющее следующим аксиомам:

- 1)  $(\forall a, b, c \in A)((a + b) + c = a + (b + c));$
- 2)  $(\forall a, b \in A)(a + b = b + a);$
- 3)  $(\exists 0 \in A)(\forall a \in A)(a + 0 = a);$
- 4)  $(\forall a \in A)(\exists (-a) \in A)(a + (-a) = 0);$
- 5)  $(\forall a, b, c \in A)(a(b + c) = ab + ac) \wedge$   
 $(\forall a, b, c \in A)((a + b)c = ac + bc);$
- 6)  $(\forall \alpha, \beta \in P)(\forall a \in A)(\alpha(\beta a) = (\alpha\beta)a);$
- 7)  $(\forall \alpha, \beta \in P)(\forall a \in A)((\alpha + \beta)a = \alpha a + \beta a);$
- 8)  $(\forall \alpha \in P)(\forall a, b \in A)(\alpha(a + b) = \alpha a + \alpha b);$
- 9)  $(\forall a \in A)(1 \cdot a = a);$
- 10)  $(\forall \alpha \in P)(\forall a, b \in A)(\alpha(ab) = (\alpha a)b = a(\alpha b)).$

Примеры алгебр.

1. Множество квадратных матриц  $M_n(P)$  – алгебра над полем  $P$ .
2.  $A = R, P = Q, R$  – алгебра действительных чисел над полем  $Q$ .

## Подалгебры

**Определение 10.** Подмножество  $S$  алгебры  $A$  над полем  $P$  называется подалгеброй алгебры  $A$ , если относительно операций, определенных в  $A$ , само множество  $S$  является алгеброй над полем  $P$ .

**Теорема 5.** (Признак подалгебры) *Непустое подмножество  $S$  алгебры  $A$  над полем  $P$  тогда и только тогда является алгеброй в  $A$ , когда выполняются следующие условия:*

- 1)  $(\forall a, b \in S)(a - b \in S)$ ;
- 2)  $(\forall a, b \in S)(ab \in S)$ ;
- 3)  $(\forall \alpha \in P)(\forall a \in S)(\alpha a \in S)$ .

Доказательство. Необходимость. Пусть  $S$  – подалгебра  $A$ . Тогда условие 1) – 3) выполняются.

Достаточность. Пусть выполняются условия 1) – 3). Тогда из условий 1) и 2) следует, что  $S$  – подкольцо кольца  $A$ , а из выполнимости условий 1) и 3) следует, что  $S$  – векторное пространство пространства  $A$ . Условие 3) определения 8 выполняется в  $S$ , так как оно верно в  $A$ , таким образом, выполняются условия 1) – 3) определения 8, следовательно,  $S$  – подалгебра алгебры  $A$ .

**Теорема 6.** Пусть  $A_i (i \in I)$  – подалгебра алгебры  $A$  над полем  $P$ . Тогда  $\bigcap_{i \in I} A_i$  – подалгебра алгебры  $A$ .

Доказательство. Пусть  $B = \bigcap_{i \in I} A_i$ . Так как каждая подалгебра  $A_i (i \in I)$  содержит нулевой элемент алгебры  $A$ , то  $B \neq \emptyset$ . Воспользуемся признаком подалгебры. Пусть  $a, b \in B$ . Тогда  $(\forall i \in I)(a, b \in A_i (i \in I))$  и потому  $a - b, ab \in A_i (i \in I)$ . Следовательно,  $a - b, ab \in B$ . Пусть  $\alpha \in P$ , тогда  $(\forall i \in I)(\alpha a \in A_i (i \in I))$ , поэтому  $\alpha a \in B$ . Таким образом,  $B$  – подалгебра алгебры  $A$ .

Пусть  $M$  – непустое подмножество алгебры  $A$  и  $\{A_i \mid i \in I\}$  – подмножество всех подалгебр алгебры  $A$ , содержащих  $M$ . Тогда согласно теореме 5,  $\bigcap_{i \in I} A_i$  – подалгебра алгебры  $A$ . Ясно, что подалгебра  $\bigcap_{i \in I} A_i$  является наименьшей из всех подалгебр, содержащих множество  $M$ .



Обозначим эту подалгебру следующим образом –  $\langle M \rangle$ . Подалгебра  $\langle M \rangle$  называется подалгеброй, порожденной множеством  $M$ , а само  $M$  называется множеством образующих алгебры  $A$ . В случае, когда множество  $M$  одноэлементное, например,  $M = \{a\}$ , подалгебру  $\langle \{a\} \rangle$  будем записывать в виде  $\langle a \rangle$  и называть моногенной или однопорожденной подалгеброй. Если в алгебре  $A$  содержится такой элемент  $a$ , что  $A = \langle a \rangle$ , то будем называть  $A$  моногенной алгеброй.

**Теорема 7.** Пусть  $A$  – алгебра над полем  $P$  и  $a \in A$ . Тогда

$$\langle a \rangle = \{\alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n \mid n \in N \text{ \& } \alpha_1, \dots, \alpha_n \in P\}.$$

Доказательство.  $\langle a \rangle$  – алгебра над полем  $P$ , тогда по определению алгебры  $a^n \in \langle a \rangle$  и  $(\forall \alpha \in P)(\alpha a \in \langle a \rangle)$ . Значит

$$\{\alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n \mid n \in N \text{ \& } \alpha_1, \dots, \alpha_n \in P\} \subseteq \langle a \rangle$$

Применяя признак подалгебры, можно убедиться в том, что подмножество  $\{\alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n \mid n \in N \text{ \& } \alpha_1, \dots, \alpha_n \in P\}$  является подалгеброй в  $A$ , содержащей элемент  $a$ . Следовательно,

$$\langle a \rangle \subseteq \{\alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n \mid n \in N \text{ \& } \alpha_1, \dots, \alpha_n \in P\}.$$

### Изоморфизм алгебр

**Определение 11.** Пусть  $A$  и  $A'$  – алгебры над полем  $P$ . Изоморфизмом алгебры  $A$  на алгебру  $A'$  назовем биективное отображение  $\varphi$  множества  $A$  на множество  $A'$ , которое удовлетворяет следующим условиям:

- 1)  $(\forall a, b \in A)(\varphi(a + b) = \varphi(a) + \varphi(b))$ ;
- 2)  $(\forall a, b \in A)(\varphi(ab) = \varphi(a)\varphi(b))$ ;
- 3)  $(\forall \alpha \in P)(\forall a \in A)(\varphi(\alpha a) = \alpha(\varphi(a)))$ ;

Замечание 3. Из условий 1) и 2) следует, что изоморфные алгебры являются изоморфными кольцами, а из условий 1) и 3) следует, что изоморфные алгебры являются изоморфными векторными пространствами.

Поэтому изоморфизмы алгебр над полем обладают всеми свойствами изоморфизмов колец и векторных пространств.

**Теорема 8.** *Любая алгебра с единицей ранга  $n$  над полем  $P$  изоморфна некоторой подалгебре алгебры матриц  $M_n(P)$ .*

Доказательство. Пусть  $A$  – алгебра ранга  $n$  над полем  $P$ . Для любого элемента  $a$  из  $A$  определим отображение  $\varphi_a: A \rightarrow A$  следующим образом:  $(\forall x \in A)(\varphi_a(x) = xa)$  и докажем, что  $\varphi_a$  – линейное отображение.

В самом деле,

$$(\forall x, y \in A)(\varphi_a(x + y) = (x + y)a = xa + ya = \varphi_a(x) + \varphi_a(y)),$$

$$(\forall x \in A)(\forall \alpha \in P)(\varphi_a(\alpha x) = (\alpha x)a = \alpha(xa) = \alpha \cdot \varphi_a(x)).$$

Подметим, что  $\varphi_{a+b} = \varphi_a + \varphi_b$ ,  $\varphi_{ab} = \varphi_a \varphi_b$ ,  $\varphi_{\alpha a} = \alpha \cdot \varphi_a$ .

Будем обозначать через  $\Phi_n$  алгебру всех линейных преобразований векторного пространства  $A$  над полем  $P$ .

Из проведенных рассуждений следует, что  $(\forall a \in A)(\varphi_a \in \Phi_n)$ .

Зададим теперь отображение  $\psi: A \rightarrow \Phi_n$  по следующему правилу:  $(\forall a \in A)(\psi(a) = \varphi_a)$  и докажем, что  $\psi$  – инъективный гомоморфизм. Действительно, пусть  $(\forall a, b \in A)$  и  $\psi(a) = \psi(b)$ . Тогда  $\varphi_a = \varphi_b$  и  $(\forall x \in A)(xa = xb)$ . Подставляя в это равенство единичный элемент алгебры  $A$ , получим, что  $a = b$ . Следовательно,  $\psi$  – инъективное отображение.

Пусть  $a, b \in A, \alpha \in P$ . Тогда

$$\psi(a + b) = \varphi_{a+b} = \varphi_a + \varphi_b = \psi(a) + \psi(b),$$

$$\psi(ab) = \varphi_{ab} = \varphi_a \varphi_b = \psi(a)\psi(b),$$

$$\psi(\alpha a) = \varphi_{\alpha a} = \alpha \varphi_a = \alpha \psi(a).$$

Следовательно,  $\psi$  – гомоморфизм. Пусть  $\psi(A)$  – гомоморфный образ алгебры  $A$ . Тогда  $\psi(A) \cong A$  и  $\psi(A)$  – подалгебра в алгебре  $\Phi_n$ . С учетом того, что  $\Phi_n \cong M_n(P)$ , получим то, что требовалось доказать.

**Теорема 9.** Пусть  $A$  – произвольная алгебра ранга  $n$  над полем  $P$ . Тогда существует алгебра  $A'$  ранга  $n+1$  с единицей над полем  $P$ , содержащая подалгебру, изоморфную алгебре  $A$ .

Доказательство. Рассмотрим множество  $A' = P \times A$  и определим на нем следующие операции:

- 1)  $(\forall \alpha, \beta \in P)(\forall a, b \in A)((\alpha, a) + (\beta, b) = (\alpha + \beta, a + b));$
- 2)  $(\forall \alpha, \beta \in P)(\forall a, b \in A)((\alpha, a)(\beta, b) = (\alpha\beta, \alpha b + \beta a + ab));$
- 3)  $(\forall \alpha, \beta \in P)(\forall a \in A)(\beta(\alpha, a) = (\beta\alpha, \beta a)).$

Легко проверяется, что  $(A', +)$  – абелева группа. Проверим выполнимость свойства дистрибутивности умножения относительно сложения:

$$\begin{aligned} (\forall \alpha, \beta, \gamma \in P)(\forall a, b, c \in A) & \left( (\alpha, a)((\beta, b) + (\gamma, c)) = (\alpha, a)(\beta + \gamma, b + c) = \right. \\ & = (\alpha(\beta + \gamma), \alpha(b + c) + (\beta + \gamma)a + a(b + c)) = \\ & = (\alpha\beta + \alpha\gamma, \alpha b + \alpha c + \beta a + \gamma a + ab + ac) = \\ & = (\alpha\beta, \alpha b + \beta a + ab) + (\alpha\gamma, \alpha c + \gamma a + ac) = \\ & \left. = (\alpha, a)(\beta, b) + (\alpha, a)(\gamma, c) \right). \end{aligned}$$

Следовательно,  $(A', +)$  – кольцо. Кроме того, не трудно проверить, что множество  $A'$  относительно операций 1) и 3) образует векторное пространство и условие 3) определения 8 также выполнимо в  $A'$ , следовательно

$$\begin{aligned} (\forall \alpha, \beta, \gamma \in P)(\forall a, b \in A) & \left( (\gamma(\alpha, a))(\beta, b) = (\gamma\alpha, \gamma a)(\beta, b) = \right. \\ & = (\gamma\alpha\beta, \gamma\alpha b + \beta\gamma a + (\gamma a)b) = \gamma(\alpha\beta, \alpha b + \beta a + ab) = \\ & \left. = \gamma((\alpha, a)(\beta, b)) = (\alpha, a)(\gamma(\beta, b)) \right). \end{aligned}$$

Таким образом,  $A'$  – алгебра над полем  $P$ . Очевидно, что элемент  $(1, 0)$ , где  $1$  – единичный элемент поля  $P$ , а  $0$  – нулевой элемент в  $A$ , является единицей этой алгебры.

Определим размерность алгебры  $A'$ . Пусть  $e_1, e_2, \dots, e_n$  – базис алгебры  $A$  (то есть базис векторного пространства  $A$  над полем  $P$ ). Тогда система

векторов  $(1,0), (0,e_1), (0,e_2), \dots, (0,e_n)$  алгебры  $A'$  линейно независима над полем  $P$ . Кроме того,

$$(\forall \alpha \in P)(\forall a \in A)(\exists \alpha_0, \alpha_1, \dots, \alpha_n \in F) \\ ((\alpha, a) = \alpha_0(1,0) + \alpha_1(0,e_1) + \dots + \alpha_n(0,e_n)).$$

Следовательно,  $A'$  – алгебра ранга  $n+1$ .

Рассмотрим теперь отображение  $\psi: A \rightarrow A'$ , определенное следующим образом:  $(\forall a \in A)(\psi(a) = (0, a))$ . Легко видеть, что  $\psi$  – инъективное отображение.

Пусть  $a, b \in A, \alpha \in F$ . Тогда

$$\begin{aligned} \psi(a+b) &= (0, a+b) = (0, a) + (0, b) = \psi(a) + \psi(b), \\ \psi(ab) &= (0, ab) = (0, a)(0, b) = \psi(a)\psi(b), \\ \psi(\alpha a) &= (0, \alpha a) = \alpha(0, a) = \alpha\psi(a). \end{aligned}$$

Следовательно,  $\psi$  – гомоморфизм и потому алгебра  $A$  изоморфна подалгебре  $\psi(A)$  алгебры  $A'$ .

Из теорем 8 и 9 вытекает следующая теорема.

**Теорема 10.** *Любая алгебра ранга  $n$  над полем  $P$  изоморфна некоторой подалгебре алгебры  $M_{n+1}(P)$ .*

## Идеалы

**Определение 12.** *Назовем подкольцо  $J$  кольца  $R$  левым (правым) идеалом, если*

$$\begin{aligned} (\forall a \in J)(\forall r \in R)(ar \in J); \\ (\forall a \in J)(\forall r \in R)(ra \in J). \end{aligned}$$

Если подкольцо  $J$  является левым и правым идеалом в  $R$ , то тогда  $J$  называется двусторонним идеалом в  $R$ .

Пусть  $A, B$  – две подгруппы в аддитивной группе  $R^+$  кольца  $R$ . Будем говорить, что кольцо  $R$  является суммой двух подгрупп  $A$  и  $B$  и писать  $R = A + B$ , если  $(\forall r \in R)(\exists a \in A)(\exists b \in B)(r = a + b)$ . Если  $R = A + B$  и  $A \cap B = \{0\}$ ,

то тогда будем обозначать  $R = A \oplus B$  и называть кольцо  $R$  разложимым в прямую сумму подгрупп (подколец). Если  $A$  и  $B$  являются двусторонними идеалами в кольце  $R$ , то тогда будем обозначать  $R = A \dot{+} B$  и называть кольцо  $R$  разложимым в прямую сумму идеалов  $A, B$ .

### Пирсовские разложения

Пусть  $R$  – произвольное кольцо. Элемент  $e \in R$  назовем идемпотентным элементом, если  $e^2 = e$ . Очевидно, что нулевой элемент кольца является идемпотентным элементом:  $0^2 = 0$ . Если кольцо  $R$  содержит единичный элемент  $1$ , то  $1$  – идемпотентный элемент.

Рассмотрим несколько типов разложений кольца  $R$  в прямую сумму своих подколец.

1)  $R = eR \oplus (1 - e)R$  – одностороннее пирсовское разложение кольца  $R$  по идемпотенту  $e$ , где  $eR = \{er | r \in R\}$ ,  $(1 - e)R = \{r - re | r \in R\}$ . Докажем, что  $eR, (1 - e)R$  – подкольца кольца  $R$ . Для этого воспользуемся признаком подкольца. Пусть  $a = er_1, b = er_2$  – произвольные элементы подмножества  $eR$ . Тогда  $a - b = er_1 - er_2 = e(r_1 - r_2) \in eR$ ;  $ab = er_1er_2 = e(r_1er_2) \in eR$ . Аналогично доказывается, что подмножество  $(1 - e)R$  есть подкольцо в  $R$ . Кроме того,  $eR \cap (1 - e)R = \{0\}$ . Легко видеть, что

$$(\forall x \in R)(x = ex + (1 - e)x = ex + x - ex).$$

Значит  $R = eR \oplus (1 - e)R$ . Ясно, что  $e$  – левая единица в подкольце  $eR$  и  $(\forall a \in (1 - e)R)(ea = e(1 - e)r = er - e^2r = er - er = 0)$ .

2)  $R = eRe \oplus eR(1 - e) \oplus (1 - e)Re \oplus (1 - e)R(1 - e)$  – двустороннее пирсовские разложения. Действительно

$$\begin{aligned} (\forall x \in R)(x &= exe + ex(1 - e) + (1 - e)xe + (1 - e)x(1 - e) = \\ &= exe + ex - exe + xe - exe + x - xe - ex + exe). \end{aligned}$$

Подмножества  $eRe, eR(1 - e), (1 - e)Re, (1 - e)R(1 - e)$  – подкольца кольца  $R$ .

3) Пусть  $e_1, e_2$  – ортогональные идемпотентные элементы кольца, то есть  $e_i^2 = e_i (i = 1, 2), e_1 e_2 = e_2 e_1 = 0$ .

Пирсовское разложение кольца  $R$  по двум ортогональным идемпотентам:

$$R = e_1 R e_1 \oplus e_1 R e_2 \oplus e_2 R e_1 \oplus e_2 R e_2 \oplus (1 - u) R (1 - u), \text{ где}$$

$$u = e_1 + e_2, u^2 = (e_1 + e_2)^2 = e_1^2 + e_1 e_2 + e_2 e_1 + e_2^2 = e_1 + e_2 = u$$

$$e_1 u = e_1 (1 - e_1 - e_2) = e_1 - e_1 = 0$$

### §3. Элементы теории решеток

#### Частично упорядоченные множества

**Определение 13.** Частично упорядоченным множеством (ч.у. множеством) называется множество, на котором определено бинарное отношение  $x \leq y$ , удовлетворяющее для всех  $x, y, z$  следующим условиям:

- 1)  $x \leq x$  (рефлексивность);
- 2) если  $x \leq y$  и  $y \leq x$ , то  $x = y$  (антисимметричность);
- 3) если  $x \leq y$  и  $y \leq z$ , то  $x \leq z$  (транзитивность).

Примеры ч.у. множеств.

1.  $M$  – любое множество с отношением  $=$ .
2.  $(N, |)$ , где  $x | y$  означает, что  $x$  делит  $y$ .

Бинарное отношение  $x \leq y$  читается как « $x$  меньше или равно  $y$ ».

Если  $x \leq y$  и  $x \neq y$ , то будем писать  $x < y$  и говорить, что « $x$  строго меньше чем  $y$ ».

Будем говорить, что элементы  $x$  и  $y$  из ч.у. множества  $(A; \leq)$  называются сравнимыми, если  $x \leq y$  или  $y \leq x$ . В противном случае  $x$  и  $y$  называются несравнимыми. Говорят, что элемент  $y$  покрывает элемент  $x$ , если  $x < y$  и

$$(\forall z \in A)((x \leq z) \wedge (z \leq y) \Rightarrow (z = x) \wedge (z = y)).$$

Используя отношение покрытия, можно следующим образом получить графическое представление любого конечного ч.у. множества  $A$ . Изобразим каждый элемент множества  $A$  в виде небольшого кружка, располагая  $y$  выше  $x$ ,

если  $x < y$ . Соединим  $x$  и  $y$  прямолинейным отрезком, если  $y$  покрывает  $x$ . Полученная фигура называется диаграммой ч.у. множества  $A$ .

**Определение 14.** *Цепь — это ч.у. множество, в котором все элементы сравнимы.*

**Определение 15.** *Антицепью называется ч.у. множество, в котором любые два различных элемента несравнимы.*

**Определение 16.** *Число  $n$  называется длиной цепи  $P$ , если  $P$  — цепь, состоящая из  $n + 1$  элемента.*

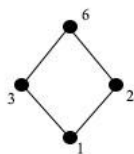
**Определение 17.** *Длиной ч.у. множества  $P$  называется целое неотрицательное число  $n$ , такое что если в  $P$  существует цепь длины  $n$  и все цепи в  $P$  имеют длину не превосходящую  $n$ .*

Если длина ч.у. множества  $P$  конечна и равна  $n$ , то  $P$  называется ч.у. множеством конечной длины  $n$ . Если же такого числа  $n$  для множества  $P$  не существует, то  $P$  называется ч.у. множеством бесконечной длины.

**Определение 18.** *Ширина ч.у. множества  $P$  равна  $n$ , где  $n$  — натуральное число, если существует антицепь в  $P$ , состоящая из  $n$  элементов, и все антицепи в  $P$  содержат не более  $n$  элементов.*

Пример.

1. Ч.у. множество — делители числа 6



Длина ч.у. множества равна 2 и ширина ч.у. множества равна 2.

**Определение 19.** *Наименьшим элементом подмножества  $X$  ч.у. множества  $P$  называется элемент  $a \in X$  такой, что  $a \leq x$  для всех  $x \in X$ . Наибольшим элементом подмножества  $X$  называется элемент  $b \in X$  такой, что  $x \leq b$  для всех  $x \in X$ .*

Будем обозначать наименьший элемент ч.у. множества цифрой 0 и называть нулем, а наибольший — цифрой 1 и называть единицей.

**Определение 20.** Минимальный элемент подмножества  $X$  ч.у. множества  $P$  — это такой элемент  $a$ , что неравенство  $x < a$  невозможно ни для какого  $x \in X$ . Максимальный элемент подмножества  $X$  ч.у. множества  $P$  — это такой элемент  $a$ , что неравенство  $a < x$  невозможно ни для какого  $x \in X$ .

**Определение 21.** Пусть  $H \subseteq P$  и  $a \in P$ . Тогда  $a$  называется верхней границей подмножества  $H$ , если  $h \leq a$  для всех  $h \in H$ .

**Определение 22.** Верхняя граница  $a$  подмножества  $H$  называется его верхней гранью или супремумом, если  $a \leq b$  для любой верхней границы  $b$  подмножества  $H$ .

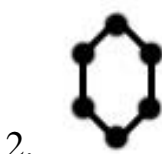
**Определение 23.** Пусть  $H \subseteq P$  и  $a \in P$ . Тогда  $a$  называется нижней границей подмножества  $H$ , если  $a \leq h$  для всех  $h \in H$ .

**Определение 24.** Нижняя граница  $a$  подмножества  $H$  называется его нижней гранью или инфимумом, если  $b \leq a$  для любой нижней границы  $b$  подмножества  $H$ .

## Основные понятия теории решеток

**Определение 25.** Решеткой (или структурой) называется ч.у. множество  $L$ , в котором любые два элемента имеют нижнюю и верхнюю грани.

Примеры решеток.



Сформулируем еще одно определение решетки как алгебры.



**Определение 26.** Множество  $L$  называется решеткой, если  $L$  — непустое множество, и на этом множестве определены бинарные операции  $\vee$  и  $\wedge$ , которые обладают свойствами:

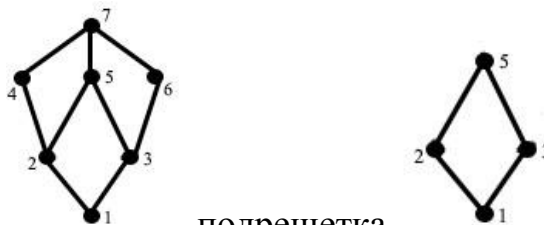
- 1)  $(\forall x \in L)(x \wedge x = x)(x \vee x = x)$  (идемпотентность);
- 2)  $(\forall x, y \in L)(x \wedge y = y \wedge x)(x \vee y = y \vee x)$  (коммутативность);
- 3)  $(\forall x, y, z \in L)(x \vee (y \vee z) = (x \vee y) \vee z)(x \wedge (y \wedge z) = (x \wedge y) \wedge z)$  (ассоциативность);
- 4)  $(\forall x, y \in L)(x \vee (x \wedge y) = x \wedge (x \vee y) = x)$  (поглощения).

### Подрешетки

**Определение 27.** Подрешеткой решетки  $L$  называется подмножество  $X \subset L$  такое, что если  $a \in X, b \in X$ , то  $a \wedge b \in X$  и  $a \vee b \in X$ .

Подрешетка решетки сама является решеткой с теми же операциями объединения и пересечения.

Пример подрешетки.



1. Решетка  $L$  имеет вид , подрешетка

**Теорема 11. (Признак подрешетки)** Непустое подмножество  $S$  решетки  $(L, \wedge, \vee)$  тогда и только тогда является подрешеткой в  $L$ , когда выполняется условие:  $(\forall x, y \in S)(x \vee y \in S \ \& \ x \wedge y \in S)$ .

Доказательство. Необходимость. Если  $S$  подрешетка решетки  $L$ , то согласно определению 26 условие  $(\forall x, y \in S)(x \vee y \in S \ \& \ x \wedge y \in S)$  выполняется.

Достаточность. Если выполняется условие  $(\forall x, y \in S)(x \vee y \in S \ \& \ x \wedge y \in S)$ , то операции  $\vee$  и  $\wedge$  определенные в  $L$ , определены и в  $S$ . Свойства идемпотентности, коммутативности, поглощения и ассоциативности для этих операций выполняются, так как они выполнимы в  $L$ .

## **ГЛАВА II. Система компьютерной алгебры GAP**

### **§ 1. Общее описание**

#### **Определение и история создания**

GAP (Groups, Algorithms and Programming) является системой компьютерной алгебры, изначально задуманной как инструмент вычислительной теории групп, и спустя некоторое время распространившейся на смежные разделы алгебры. Создание и первоначальные разработки GAP проходили в Германии в городе Аахен (Lehrstuhl D für Mathematik, RWTH). В данный момент, техническая поддержка и центр разработки GAP находится в Шотландии (School of Mathematical and Computational Sciences, University of St.-Andrews).

Внешне язык программирования системы GAP напоминает Паскаль, что очень удобно, так как этот язык изучают в школе и поэтому на психологическом уровне пользователю становится комфортнее работать. Так же GAP можно бесплатно получить по сети Internet вместе с исходными текстами, являющимися незаменимым наглядным пособием для освоения GAP.

На данный момент существует уже более 20 версий системы GAP, последняя версия GAP 4.8.6 была выпущена в ноябре 2016 года.

#### **Системные требования**

Один из главных плюсов компьютерной системы GAP это не высокие системные требования. Данная программа совместима с такими операционными системами как: DOS, Windows, Unix, Linux, MacOS и поддерживает работу с процессором типа 386 и выше с оперативной памятью от 8 мегабит.

Компактная программа, которая требует всего свободного места на диске от 10 до 100 мегабит, в зависимости от объема инсталляции.

## **Этапы установки**

1. Выберите нужный формат архива и скачайте соответствующий архив.
2. Распакуйте архив.
3. В UNIX, Linux или Mac OS X нужно скомпилировать ядро GAP системы. Затем зайти в подкаталог и вызвать скрипт, который будет создавать большую часть пакетов, которые требуют компиляций.
4. В Windows программа не требует компиляции, скомпилированные файлы для GAP и некоторые пакеты уже находятся в win.zip-архиве.
5. Отрегулировать некоторые ссылки, скрипты, значки в зависимости от системы, чтобы сделать версию GAP доступной пользователю.

## **Справочная система GAP и основные алгебраические системы**

GAP – универсальная программа позволяющая работать с различными объектами и алгебраическими системами такими как: целые числа, рациональные числа, массивы, векторные и матричные объекты, отношения и отображения, группы, кольца, поля, векторные пространства, алгебры и т.д.

Для комфортной работы пользователей и знакомства с компьютерной системой GAP официальный сайт <https://www.gap-system.org> предоставляет справочник Reference Manual. Данное системное руководство является обще доступным ресурсом в открытом доступе сети Интернет. Справочник содержит введение в систему и полное описанием всех функций, библиотек и предоставляет примеры их использования. Удобное оформление позволяет свободно передвигаться по справочнику, с легкостью попадая в любой раздел. Также в документе под названием Changes from Earlier Versions описаны наиболее важные изменения по сравнению с предыдущими выпусками GAP.

Каждый пакет GAP имеет свое индивидуальное руководство, которое можно получить на сайте в разделе Packages. Список указателей на все эти пакеты руководства также приведен на странице Manuals.

## § 2. Язык программирования GAP

Ввод GAP состоит из последовательностей следующих символов: цифры, латинские буквы верхнего и нижнего регистра, пробел, символ табуляции, символ начала строки, 24 специальных символов ( “ ’ ( ) \* + , \_ . / : ; < = > ~ [ \ ] ^ \_ { } # ), остальные символы будут сигнализироваться как запрещенные.

Набор лексических единиц состоит из: ключевых слов, идентификаторов, строк, целых чисел, символов операторов, символов разделителя.

### Ключевые слова

Ключевыми словами являются зарезервированные слова, которые используются, чтобы обозначать специальные операции. Важным правилом является то, что ключевые слова не должны содержать пробелов и не должны использоваться как идентификаторы.

Список ключевых слов:

and	until	od	if	else	end	fi
for	do	while	or	in	local	mod
not	function	elif	quit	repeat	return	then

### Идентификаторы

Идентификатор состоит из цифр, букв и знака подчеркивания, причем хотя бы из одного. Наклонная черта/ может использоваться, чтобы включить другие символы в идентификаторы.

### Выражения

Переменные, вызовы функций, целые числа, подстановки, строки, функции и списки являются самыми простыми случаями выражений. Более сложные выражения могут быть составлены из них объединения с помощью операторов нескольких простых. Существует три класса операторов: сравнения ( = < > <= >= in ), арифметические ( + − \* / mod ^ ) и логические ( not and or ).

### § 3. Основные команды, используемые в работе

Название команды	Описание
<code>Genm:=[];</code>	Создает каталог для размещения информации;
<code>MatAlgebra (GF (M) , N) ;</code>	Строит алгебру матриц n-ого порядка над полем GF(M);
<code>Subalgebra (A, El[i]) ;</code>	Строит моногенную подалгебру алгебры A;
<code>Elements (A) ;</code>	Создает массив элементов алгебры A;
<code>Dimension (A) ;</code>	Считает размерность алгебры A;
<code>PrintTo ("имя_файла.расширение", "результат") ;</code>	Печатает результата в файл;
<code>PrintArray (A) ;</code>	Выдает на экран матрицу A построчно;
<code>LogTo ("имя_файла.расширение") ;</code>	Записывает в указанный файл все, что будет выведено на экран после этой команды;
<code>Size (A) ;</code>	Считает размер матрицы A;
<code>Add (A, i) ;</code>	Добавляет в A значение переменной i;
<code>AddSet (A, i) ;</code>	Добавляет в массив A новый элемент i;
<code>Read ("имя_файла.расширение") ;</code>	Читает указанный файл;
<code>Sort (A) ;</code>	Упорядочивает по возрастанию элементы массива A;
<code>SubtractSet (A, [i]) ;</code>	Удаляет из массива A элемент i
<code>Position (A, i) ;</code>	Определяет номер элемента i в массиве A;
<code>IntersectSet (A, B) ;</code>	Находит пересечение множества a и B;
<code>UniteSet (A, B) ;</code>	Находит объединение множества a и B;
<code>SubtractSet (A, B) ;</code>	Удаляет из множества A все элементы множества B;
<code>for _ in _ do _; od;</code>	Задание цикла;
<code>if _ then _; fi;</code>	Проверка условия;
<code>quit;</code>	Выход из программы.

## § 4. Простейшие программы вычислений в матричной алгебре

### Программа создание массива порождающих элементов.

```
A:=MatAlgebra(GF(2),3);;
El:=Elements(A);;
B:=[];
C:=[];
for i in [1..512] do
S:=Subalgebra(A,[El[i]]);
el:=Elements(S);
a:=Size(B);
AddSet(B,el);
b:=Size(B);
if b>a then
Add(C,i);
fi;
od;
PrintTo("Dann.dan","Gen:=",C,"");
```

### Программа для составления таблиц сложения и умножения.

```
A:=MatAlgebra(GF(2),3);;
El:=Elements(A);;
sum:=[];
prod:=[];
for i in [1..16] do
sum[i]:=[];
prod[i]:=[];
for j in [1..16] do
sum[i][j]:=Position(El,El[i]+El[j]);
prod[i][j]:=Position(El,El[i]*El[j]);
od;od;
PrintTo("sum:", "\n", sum, "\n", "prod:", "\n", prod, "\n");
```

## ГЛАВА III. Исследования конечномерных алгебр

### §1. Тип решетки

Пусть  $A = M_3(GF(2))$ . Алгебра  $A$  содержит  $2^9 = 512$  элементов. Количество подалгебр равняется 2102 [7]. На данный момент классифицированы все подалгебры порожденные одним элементом [8] алгебры  $A$ , двухмерные, трехмерные [9]. Количество четырехмерных подалгебр равняется 497 [7], но их решетки до настоящего времени оставались неизученными.

Введем понятие типа решетки для подалгебр алгебры  $A$ .

**Определение 28.** Пусть  $S$  – подалгебра порядка  $2^n$  алгебры  $M_3(GF(2))$ . Упорядоченная последовательность  $(m_0, m_1, \dots, m_n)$  называется типом решетки подалгебр алгебры  $S$ , если  $m_i$  – число подалгебр в  $S$  порядка  $2^i$ , где  $i = \overline{0, n}$ .

### §2. Алгоритм исследования четырехмерных подалгебр

Поставленная ранее задача получить классификацию по типам решеток с точностью до изоморфизма алгебр, решается с помощью следующего алгоритма:

1. Исходя из пирсовского разложения алгебры по одному, двум, и трем идемпотентным элементам, выбираем базис из четырех элементов. Как правило, в качестве базисных переменных выбираем идемпотентные и нильпотентные элементы индекса 2. После выбора базиса составляем таблицу умножения.

2. Находим в алгебре  $A$  все подалгебры с заданной таблицей умножения. Ясно, что все такие подалгебры изоморфны между собой, следовательно, имеют один и тот же тип решетки подалгебр. При этом может оказаться, что подалгебр с данной таблицей умножения не существует.

Приведем пример программы, с помощью которой решается рассмотренная задача.

**Программа нахождения четырехмерных подалгебр с заданной таблицей умножения.**

```
eerr:=[];
Sub:=[]; b:=0;
Num:=[];
ID:=[2,4,6,8,10,17,18,19,22,25,46,49,50,54,55,57,66,74,82,
122,145,146,147,152,196,210,217,239,257,258,260,261,266,273,
274,275,277,279,281,289,290,293,296,298,317,321,337,345,361,
385,386,388,391,449,458,467,512];
NI:=[3,5,7,9,28,33,37,41,64,65,73,129,131,193,220,326,366,
433,439,456,505];
A:=MatAlgebra(GF(2),3);
El:=Elements(A);
  for i in ID do
    for j in ID do
      for k in NI do
        for l in NI do
if j<>i and l<>k and
  El[i]*El[j]=El[1] and El[j]*El[i]=El[1] and
  El[i]*El[k]=El[k] and El[k]*El[i]=El[1] and
  El[i]*El[l]=El[1] and El[l]*El[i]=El[1] and
  El[j]*El[k]=El[1] and El[k]*El[j]=El[k] and
  El[j]*El[l]=El[1] and El[l]*El[j]=El[1] and
  El[l]*El[k]=El[1] and El[k]*El[l]=El[1] then
B:=Subalgebra(A,[El[i],El[j],El[k],El[l]]);
sub:=Elements(B);
AddSet(Sub,sub);
if Size(Sub)>b then
Add(eerr,[i,j,k,l]);
b:=Size(Sub);
fi;fi;od;od;od;od;
```



```

Str:=[];
for t in [1..16] do
Add(Str, Position(El,sub[t]));
Add(Num, Str);
od;
Sort(eerr);
PrintTo("eerr-1.dan", "eerr:=", eerr, ";", "\n", "|eerr|=",
Size(eerr), "\n");
PrintTo("Sub-1.dan", "Sub-1:=", Sub, ";", "\n");

```

3. Для полученного множества попарно изоморфных алгебр определяем их тип решетки подалгебр. Приведем пример программы, с помощью которой решается рассмотренная задача.

### **Программа нахождения типа решетки подалгебр.**

```

tip:=function(a,b,c,d)
local sub,A,tip,El,S,i,s,j,el,k,y,l;
sub:=[];
tip:=[];
A:=MatAlgebra(GF(2),3);
El:=Elements(A);
S:=Subalgebra(A,[El[a],El[b],El[c],El[d]]);
for i in S do
for k in S do
for j in S do
for y in S do
S:=Subalgebra(A,[i,j,k,y]);
AddSet(sub, Elements(S));
od;
od;
od;
od;
for l in [1..Size(sub)] do
Add(tip, Size(sub[l]));
od;

```

```

tip:=Collected(tip);
PrintTo("tip.dan", " a= ",a,";", " b= ",b,";", " c= ",c,";",
"d= ",d,";", "\n",tip);
end;

```

После запуска программы в командную строку нужно ввести  $\text{tip}(a, b, c, d)$ ; где  $(a, b, c, d)$  – четверка номеров матриц, порождающих данную подалгебру, полученную на втором этапе алгоритма.

4. Если ранее уже были найдены подалгебры с данным типом решетки, то выясняем, являются ли эти подалгебры новыми или изоморфными предыдущим. Если получили новые подалгебры, то пополняем общую таблицу результатов. Проверка на изоморфизм осуществляется при помощи двух программ. Первая программа записывает в документ формата \*.dan номера всех матриц, которые порождают подалгебры, полученные на третьем шаге алгоритма.

#### **Программа нахождения номеров матриц.**

```

Num:=[];
eerr:=[[2,17,3,5], [2,49,7,5], [2,145,3,7], [2,257,5,3],
[2,289,5,7], [2,385,7,3], [10,25,28,37], [10,57,64,37],
[10,217,28,64], [10,257,37,28], [10,289,37,64],
[10,449,64,28], [17,2,9,33], [17,6,41,33], [17,66,9,41],
[17,257,33,9], [17,261,33,41], [17,321,41,9],
[66,17,131,326], [66,57,456,326], [66,145,131,456],
[66,321,326,131], [66,361,326,456], [66,449,456,131],
[74,25,220,366], [74,49,439,366], [74,217,220,439],
[74,321,366,220], [74,361,366,439], [74,385,439,220],
[145,2,73,433], [145,8,505,433], [145,66,73,505],
[145,385,433,73], [145,391,433,505], [145,449,505,73],
[257,2,65,129], [257,4,193,129], [257,10,65,193],
[257,17,129,65], [257,19,129,193], [257,25,193,65]];
A:=MatAlgebra(GF(2),3);
El:=Elements(A);
for i in [1..42] do

```

```

      B:=Subalgebra(A,[El[eerr[i][1]],El[eerr[i][2]],El[eerr[i][3]]
,El[eerr[i][4]]]);
      sub:=Elements(B);
      num:=[];
      for j in [1..16] do
      Add(num,Position(El,sub[j]));
      od;
      AddSet(Num,num);
      od;
      PrintTo("S1.dan","S1:=",Num,";","\n");

```

Вторая программа находит пересечение массивов номеров матриц, порождающих алгебры с одинаковым типом решетки. Приведем пример программы, с помощью которой решается рассмотренная задача.

### **Программа нахождения пересечения массивов.**

```

S1:=[ [1,2,3,4,5,6,7,8,17,18,19,20,21,22,23,24],
[1,2,3,4,5,6,7,8,49,50,51,52,53,54,55,56],
[1,2,3,4,5,6,7,8,145,146,147,148,149,150,151,152],
[1,2,3,4,5,6,7,8,257,258,259,260,261,262,263,264],
[1,2,3,4,5,6,7,8,289,290,291,292,293,294,295,296],
[1,2,3,4,5,6,7,8,385,386,387,388,389,390,391,392],
[1,2,9,10,17,18,25,26,33,34,41,42,49,50,57,58],
[1,2,65,66,129,130,193,194,257,258,321,322,385,386,449,450],
[1,2,73,74,145,146,217,218,289,290,361,362,433,434,505,506],
[1,4,10,11,18,19,25,28,37,40,46,47,54,55,61,64],
[1,4,65,68,129,132,193,196,257,260,321,324,385,388,449,452],
[1,4,74,75,146,147,217,220,293,296,366,367,438,439,509,512],
[1,6,9,14,17,22,25,30,33,38,41,46,49,54,57,62],
[1,6,66,69,131,136,196,199,258,261,321,326,388,391,451,456],
[1,6,74,77,147,152,220,223,290,293,361,366,436,439,507,512],
[1,8,10,15,19,22,28,29,36,37,43,46,50,55,57,64],
[1,8,66,71,131,134,196,197,260,261,323,326,386,391,449,456],
[1,8,73,80,145,152,217,224,289,296,361,368,433,440,505,512],
[1,9,17,25,33,41,49,57,66,74,82,90,98,106,114,122],
[1,9,17,25,33,41,49,57,257,265,273,281,289,297,305,313],
[1,9,17,25,33,41,49,57,261,269,277,285,293,301,309,317],
[1,9,17,25,33,41,49,57,321,329,337,345,353,361,369,377],
[1,10,19,28,37,46,55,64,196,203,210,217,232,239,246,253],
[1,10,19,28,37,46,55,64,257,266,275,284,293,302,311,320],
[1,10,19,28,37,46,55,64,261,270,279,288,289,298,307,316],
[1,10,19,28,37,46,55,64,449,458,467,476,485,494,503,512],
[1,10,65,74,129,138,193,202,257,266,321,330,385,394,449,458],
[1,10,66,73,145,154,210,217,289,298,354,361,433,442,498,505],
[1,17,65,81,129,145,193,209,257,273,321,337,385,401,449,465],

```

[1,17,66,82,131,147,196,212,261,277,326,342,391,407,456,472],  
 [1,19,65,83,129,147,193,211,257,275,321,339,385,403,449,467],  
 [1,19,66,84,131,145,196,210,261,279,326,344,391,405,456,470],  
 [1,25,65,89,129,153,193,217,257,281,321,345,385,409,449,473],  
 [1,25,74,82,139,147,196,220,293,317,366,374,431,439,488,512],  
 [1,46,66,109,131,176,196,239,261,298,326,361,391,428,456,491],  
 [1,46,74,101,147,192,220,247,266,293,321,366,412,439,467,512],  
 [1,49,73,121,145,161,217,233,273,289,345,361,385,433,457,505],  
 [1,49,74,122,147,163,220,236,277,293,350,366,391,439,464,512],  
 [1,55,73,127,145,167,217,239,279,289,351,361,391,433,463,505],  
 [1,55,74,128,147,165,220,238,275,293,348,366,385,439,458,512],  
 [1,57,66,122,131,187,196,252,261,317,326,382,391,447,456,512],  
 [1,57,73,113,145,169,217,225,281,289,337,361,393,433,449,505]];

S2:=[ [1,2,3,4,17,18,19,20,129,130,131,132,145,146,147,148],  
 [1,2,5,6,33,34,37,38,257,258,261,262,289,290,293,294],  
 [1,2,7,8,49,50,55,56,385,386,391,392,433,434,439,440],  
 [1,2,9,10,17,18,25,26,65,66,73,74,81,82,89,90],  
 [1,2,9,10,49,50,57,58,65,66,73,74,113,114,121,122],  
 [1,2,9,10,65,66,73,74,145,146,153,154,209,210,217,218],  
 [1,2,9,10,65,66,73,74,257,258,265,266,321,322,329,330],  
 [1,2,9,10,65,66,73,74,289,290,297,298,353,354,361,362],  
 [1,2,9,10,65,66,73,74,385,386,393,394,449,450,457,458],  
 [1,3,6,8,17,19,22,24,129,131,134,136,145,147,150,152],  
 [1,3,17,19,66,68,82,84,129,131,145,147,194,196,210,212],  
 [1,3,17,19,129,131,145,147,257,259,273,275,385,387,401,403],  
 [1,3,17,19,129,131,145,147,261,263,277,279,389,391,405,407],  
 [1,3,17,19,129,131,145,147,321,323,337,339,449,451,465,467],  
 [1,4,5,8,33,36,37,40,257,260,261,264,289,292,293,296],  
 [1,4,6,7,49,52,54,55,385,388,390,391,433,436,438,439],  
 [1,4,10,11,18,19,25,28,193,196,202,203,210,211,217,220],  
 [1,4,25,28,46,47,54,55,193,196,217,220,238,239,246,247],  
 [1,4,25,28,74,75,82,83,138,139,146,147,193,196,217,220],  
 [1,4,25,28,193,196,217,220,257,260,281,284,449,452,473,476],  
 [1,4,25,28,193,196,217,220,293,296,317,320,485,488,509,512],  
 [1,4,25,28,193,196,217,220,321,324,345,348,385,388,409,412],  
 [1,5,10,14,33,37,42,46,257,261,266,270,289,293,298,302],  
 [1,5,17,21,33,37,49,53,257,261,273,277,289,293,305,309],  
 [1,5,19,23,33,37,51,55,257,261,275,279,289,293,307,311],  
 [1,5,25,29,33,37,57,61,257,261,281,285,289,293,313,317],  
 [1,6,17,22,41,46,57,62,321,326,337,342,361,366,377,382],  
 [1,6,25,30,41,46,49,54,321,326,345,350,361,366,369,374],  
 [1,6,41,46,66,69,106,109,258,261,298,301,321,326,361,366],  
 [1,6,41,46,74,77,98,101,266,269,290,293,321,326,361,366],  
 [1,6,41,46,147,152,187,192,321,326,361,366,467,472,507,512],  
 [1,6,41,46,196,199,236,239,321,326,361,366,388,391,428,431],  
 [1,7,49,55,74,80,122,128,385,391,433,439,458,464,506,512],  
 [1,7,49,55,145,151,161,167,273,279,289,295,385,391,433,439],  
 [1,7,49,55,147,149,163,165,275,277,291,293,385,391,433,439],  
 [1,7,49,55,217,223,233,239,345,351,361,367,385,391,433,439],  
 [1,8,10,15,50,55,57,64,449,456,458,463,498,503,505,512],

[1, 8, 19, 22, 43, 46, 57, 64, 449, 456, 467, 470, 491, 494, 505, 512],  
 [1, 8, 57, 64, 66, 71, 122, 127, 386, 391, 442, 447, 449, 456, 505, 512],  
 [1, 8, 57, 64, 145, 152, 169, 176, 337, 344, 361, 368, 449, 456, 505, 512],  
 [1, 8, 57, 64, 196, 197, 252, 253, 260, 261, 316, 317, 449, 456, 505, 512],  
 [1, 8, 57, 64, 217, 224, 225, 232, 281, 288, 289, 296, 449, 456, 505, 512]];

Далее запускается программа и прописывается команда `Intersection(S1, S2)`, после выполнения которой, на экран выводится пересечение данных двух массивов. Если пересечение равняется пустому множеству, то тогда мы получили новые алгебры.

5. Если общее количество полученных подалгебр достигает числа 497, то это означает, что все четырехмерные подалгебры классифицированы по типам решеток.

6. Для каждого полученного типа строим диаграмму решетки подалгебры, если для данного типа существует несколько не изоморфных между собой подалгебр, то для каждого попарно изоморфного подмножества строим решетки, и с помощью диаграмм отвечаем на вопрос об изоморфизме самих решеток внутри одного типа.

Анализ различных вариантов таблиц умножения, оказался очень трудоемким, так как не всегда новые таблицы умножения приводят к новым алгебрам. Работа проводилась совместно со студентом группы Б-42 Бурдыко Виталием. В результате исследования получена полная классификация четырехмерных подалгебр по типам решеток. Эта классификация представлена в таблице 5.

Таблица 4. Общая таблица классификации четырехмерных подалгебр

№	Тип решетки	Число подалгебр в подалгебре данного типа	Моногенные	Количество подалгебр данного типа	Количество подалгебр данной размерности
Четырехмерные					
1	(1,6,8,4,1)	20	—	21	497
2	(1,7,11,1,1)	21	—	14	
3	(1,8,12,6,1)	28	—	84	
4	(1,9,11,5,1)	27	—	42	

5	(1,9,13,4,1)	28	—	84	
6	(1,10,13,3,1)	28	—	28	
7	(1,11,17,7,1)	37	—	126	
8	(1,12,18,8,1)	40	—	84	
9	(1,12,20,9,1)	43	—	14	

В данной дипломной работе представлены алгебры с типами решеток (1,6,8,4,1), (1,9,11,5,1), (1,9,13,4,1), (1,12,18,8,1), (1,12,20,9,1).

Основные результаты исследования содержатся в сформулированных далее пяти теоремах. Доказательство следующих теорем осуществляются с помощью программ построенных на основе алгоритма исследования четырехмерных подалгебр. Отличия этих программ состоят в блоках, задающих умножения в соответствующей алгебре и в номерах порождающих матриц рассматриваемую алгебру.

**Теорема 1.** В алгебре матриц  $A = M_3(GF(2))$ , содержится точно 21 подалгебра имеющая тип решетки (1,6,8,4,1). Все такие подалгебры изоморфны между собой, порождаются элементами  $e, r_1, r_2$  и имеют следующую таблицу умножения:

Таблица 5.

·	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_1$
$r_2$	0	0	$r_2$
$e$	$r_1$	$r_2$	$e$

Получен результат в виде массива номеров троек базисных элементов.

err1:= [ [ 13, 5, 274 ], [ 32, 5, 274 ], [ 35, 33, 274 ], [ 67, 3, 274 ],  
[ 79, 7, 274 ], [ 92, 28, 274 ], [ 97, 65, 274 ], [ 120, 64, 274 ], [ 133, 129, 274 ],  
[ 137, 9, 274 ], [ 171, 41, 274 ], [ 190, 64, 274 ], [ 222, 7, 274 ], [ 229, 193, 274 ],  
[ 244, 41, 274 ], [ 328, 3, 274 ], [ 334, 326, 274 ], [ 375, 28, 274 ], [ 435, 433, 274 ],  
[ 441, 9, 274 ], [ 477, 456, 274 ] ];

|err1|=21

**Теорема 2.** В алгебре матриц  $A = M_3(GF(2))$ , содержится точно 42 подалгебры имеющих тип решетки (1,9,11,5,1). Все такие подалгебры

изоморфны между собой, порождаются элементами  $e, r_1, r_2$  и имеют следующие таблицы умножения:

Таблица 6.

$\cdot$	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$
$r_2$	0	0	0
$e$	$r_2$	$r_2$	$e$

Таблица 7.

$\cdot$	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_2$
$r_2$	0	0	$r_2$
$e$	$r_1 + r_2$	0	$e$

Получен результат в виде массива номеров троек базисных элементов.

err1:= [ [ 13, 5, 2 ], [ 32, 5, 4 ], [ 35, 33, 17 ], [ 67, 3, 2 ], [ 79, 7, 2 ],  
[ 92, 28, 10 ], [ 97, 65, 257 ], [ 120, 64, 10 ], [ 133, 129, 257 ], [ 137, 9, 17 ],  
[ 171, 41, 17 ], [ 190, 64, 19 ], [ 222, 7, 4 ], [ 229, 193, 257 ], [ 244, 41, 25 ],  
[ 328, 3, 6 ], [ 334, 326, 66 ], [ 375, 28, 46 ], [ 435, 433, 145 ], [ 441, 9, 49 ],  
[ 477, 456, 196 ] ];

| err1|=21

err2:= [ [ 13, 5, 273 ], [ 32, 5, 275 ], [ 35, 33, 258 ], [ 67, 3, 273 ], [ 79, 7, 273 ],  
[ 92, 28, 281 ], [ 97, 65, 18 ], [ 120, 64, 281 ], [ 133, 129, 18 ], [ 137, 9, 258 ],  
[ 171, 41, 258 ], [ 190, 64, 260 ], [ 222, 7, 275 ], [ 229, 193, 18 ], [ 244, 41, 266 ],  
[ 328, 3, 277 ], [ 334, 326, 337 ], [ 375, 28, 317 ], [ 435, 433, 386 ], [ 441, 9, 290 ],  
[ 477, 456, 467 ] ];

| err2|=21

**Теорема 3.** В алгебре матриц  $A = M_3(GF(2))$ , содержится точно 84 подалгебры имеющих тип решетки (1,9,13,4,1). Все такие подалгебры изоморфны между собой, порождаются элементами  $e, r_1, r_2$  и имеют следующие таблицы умножения:

Таблица 8.

·	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$
$r_2$	0	0	0
$e$	$r_1$	$r_2$	$e$

Таблица 9.

·	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$
$r_2$	0	0	0
$e$	$r_1$	$r_2$	$e$

Таблица 10.

·	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	$r_1$
$r_2$	0	0	$r_2$
$e$	$r_2$	$r_2$	$e$

Таблица 11.

·	$r_1$	$r_2$	$e$
$r_1$	$r_1^2$	$r_1^2$	0
$r_2$	0	0	0
$e$	$r_1 + r_2$	0	$e$

Получен результат в виде массива номеров троек базисных элементов.

```
err1:= [ [ 13, 5, 18 ], [ 32, 5, 18 ], [ 35, 33, 18 ], [ 67, 3, 258 ], [ 79, 7, 146 ],
[ 92, 28, 266 ], [ 97, 65, 273 ], [ 120, 64, 210 ], [ 133, 129, 258 ], [ 137, 9, 273 ],
[ 171, 41, 82 ], [ 190, 64, 210 ], [ 222, 7, 146 ], [ 229, 193, 266 ], [ 244, 41, 82 ],
[ 328, 3, 258 ], [ 334, 326, 82 ], [ 375, 28, 266 ], [ 435, 433, 146 ], [ 441, 9, 273 ],
[ 477, 456, 210 ] ];
```

```
| err1|=21
```

```
err2:= [ [ 13, 5, 257 ], [ 32, 5, 257 ], [ 35, 33, 257 ], [ 67, 3, 17 ], [ 79, 7, 49 ],
[ 92, 28, 25 ], [ 97, 65, 2 ], [ 120, 64, 57 ], [ 133, 129, 17 ], [ 137, 9, 2 ], [ 171, 41, 6 ],
[ 190, 64, 8 ], [ 222, 7, 55 ], [ 229, 193, 4 ], [ 244, 41, 46 ], [ 328, 3, 17 ],
[ 334, 326, 321 ], [ 375, 28, 25 ], [ 435, 433, 385 ], [ 441, 9, 2 ], [ 477, 456, 449 ] ];
```

```
| err2|=21
```



err3:= [ [ 13, 5, 258 ], [ 32, 5, 260 ], [ 35, 33, 273 ], [ 67, 3, 18 ], [ 79, 7, 50 ],  
 [ 92, 28, 18 ], [ 97, 65, 258 ], [ 120, 64, 50 ], [ 133, 129, 273 ], [ 137, 9, 18 ],  
 [ 171, 41, 22 ], [ 190, 64, 22 ], [ 222, 7, 54 ], [ 229, 193, 260 ], [ 244, 41, 54 ],  
 [ 328, 3, 22 ], [ 334, 326, 258 ], [ 375, 28, 54 ], [ 435, 433, 273 ], [ 441, 9, 50 ],  
 [ 477, 456, 260 ] ];

| err3|=21

err4:= [ [ 13, 5, 17 ], [ 32, 5, 19 ], [ 35, 33, 2 ], [ 67, 3, 257 ], [ 79, 7, 145 ],  
 [ 92, 28, 257 ], [ 97, 65, 17 ], [ 120, 64, 217 ], [ 133, 129, 2 ], [ 137, 9, 257 ],  
 [ 171, 41, 66 ], [ 190, 64, 196 ], [ 222, 7, 147 ], [ 229, 193, 10 ], [ 244, 41, 74 ],  
 [ 328, 3, 261 ], [ 334, 326, 17 ], [ 375, 28, 293 ], [ 435, 433, 2 ], [ 441, 9, 289 ],  
 [ 477, 456, 19 ] ];

| err4|=21

**Теорема 4.** В алгебре матриц  $A = M_3(GF(2))$ , содержится точно 84 подалгебры имеющих тип решетки (1,12,18,8,1). Все такие подалгебры изоморфны между собой, порождаются элементами  $r, e_1, e_2, e_3$  и имеют следующие таблицы умножения:

Таблица 12.

·	$e_1$	$e_2$	$e_3$	$r$
$e_1$	e	0	0	r
$e_2$	0	0	0	0
$e_3$	0	0	0	0
$r$	0	0	r	0

Получен результат в виде массива номеров четверок базисных элементов.

eeer1:= [ [ 2, 17, 257, 5 ], [ 2, 49, 289, 5 ], [ 2, 145, 385, 7 ], [ 2, 257, 17, 3 ],  
 [ 2, 289, 49, 7 ], [ 2, 385, 145, 3 ], [ 4, 19, 257, 5 ], [ 4, 55, 293, 5 ], [ 4, 147, 385, 7 ],  
 [ 4, 293, 55, 7 ], [ 6, 261, 17, 3 ], [ 6, 391, 147, 3 ], [ 10, 25, 257, 37 ],  
 [ 10, 57, 289, 37 ], [ 10, 217, 449, 64 ], [ 10, 257, 25, 28 ], [ 10, 289, 57, 64 ],  
 [ 10, 449, 217, 28 ], [ 17, 2, 257, 33 ], [ 17, 6, 261, 33 ], [ 17, 66, 321, 41 ],

[ 17, 257, 2, 9 ], [ 17, 261, 6, 41 ], [ 17, 321, 66, 9 ], [ 19, 4, 257, 37 ],  
 [ 19, 8, 261, 37 ], [ 19, 196, 449, 64 ], [ 19, 261, 8, 64 ], [ 25, 10, 257, 33 ],  
 [ 25, 46, 293, 33 ], [ 25, 74, 321, 41 ], [ 25, 293, 46, 41 ], [ 46, 293, 25, 28 ],  
 [ 46, 512, 196, 28 ], [ 49, 289, 2, 9 ], [ 49, 361, 74, 9 ], [ 66, 17, 321, 326 ],  
 [ 66, 57, 361, 326 ], [ 66, 145, 449, 456 ], [ 66, 321, 17, 131 ], [ 66, 361, 57, 456 ],  
 [ 66, 449, 145, 131 ], [ 74, 25, 321, 366 ], [ 74, 49, 361, 366 ], [ 74, 217, 385, 439 ],  
 [ 74, 321, 25, 220 ], [ 74, 361, 49, 439 ], [ 74, 385, 217, 220 ], [ 145, 2, 385, 433 ],  
 [ 145, 8, 391, 433 ], [ 145, 66, 449, 505 ], [ 145, 385, 2, 73 ], [ 145, 391, 8, 505 ],  
 [ 145, 449, 66, 73 ], [ 147, 4, 385, 439 ], [ 147, 6, 391, 439 ], [ 147, 196, 321, 366 ],  
 [ 147, 391, 6, 366 ], [ 196, 19, 449, 456 ], [ 196, 46, 512, 456 ], [ 196, 147, 321, 326 ],  
 [ 196, 512, 46, 326 ], [ 217, 10, 449, 505 ], [ 217, 55, 512, 505 ], [ 217, 74, 385, 433 ],  
 [ 217, 512, 55, 433 ], [ 257, 2, 17, 129 ], [ 257, 4, 19, 129 ], [ 257, 10, 25, 193 ],  
 [ 257, 17, 2, 65 ], [ 257, 19, 4, 193 ], [ 257, 25, 10, 65 ], [ 261, 6, 17, 131 ],  
 [ 261, 8, 19, 131 ], [ 289, 49, 2, 73 ], [ 289, 57, 10, 73 ], [ 293, 46, 25, 220 ],  
 [ 293, 55, 4, 220 ], [ 321, 66, 17, 129 ], [ 321, 74, 25, 193 ], [ 321, 147, 196, 193 ],  
 [ 321, 196, 147, 129 ], [ 385, 145, 2, 65 ], [ 385, 217, 74, 65 ]];

$$|ceer1|=84$$

**Теорема 5.** В алгебре матриц  $A = M_3(GF(2))$ , содержится точно 14 подалгебр имеющих тип решетки  $(1,12,20,9,1)$ . Все такие подалгебры изоморфны между собой, порождаются элементами  $r_1, r_2, e_1, e_2$  и имеют следующие таблицы умножения:

Таблица 13.

·	$e_1$	$e_2$	$r_1$	$r_2$
$e_1$	$e_1$	0	$r_1$	$r_2$
$e_2$	0	$e_2$	0	0
$r_1$	0	$r_1$	0	0
$r_2$	0	$r_2$	0	0

Получен результат в виде массива номеров четверок базисных элементов.

```
eerr:=[ [ 2, 273, 3, 5 ], [ 10, 281, 28, 37 ], [ 17, 258, 9, 33 ], [ 18, 257, 5, 33 ],
[ 66, 337, 131, 326 ], [ 74, 345, 220, 366 ], [ 82, 321, 41, 326 ], [ 145, 386, 73, 433 ],
[ 146, 385, 7, 433 ], [ 210, 449, 64, 456 ], [ 257, 18, 65, 129 ], [ 258, 17, 3, 129 ],
[ 266, 25, 28, 193 ], [ 273, 2, 9, 65 ]];
```

```
|eerr|=14
```

### **§3. Алгоритм построения диаграммы решетки подалгебры.**

Пусть требуется построить диаграмму решетки подалгебр подалгебры  $S$  алгебры  $A$ . Построения диаграммы состоит из следующих шагов:

*Шаг 1.* Создается массив  $sub$ , в который будет содержать все подалгебры алгебры  $S$ .

*Шаг 2.* Массив  $sub$  разбивается на пять подмассивов соответствующих размерностям подалгебр.

*Шаг 3.* Создается вся алгебра  $A$  и массив ее элементов.

*Шаг 4.* Выбирается базис подалгебры  $S$  и строится сама алгебра  $S$  и массив ее элементов.

*Шаг 5.* С помощью нескольких циклов строятся все подалгебры алгебры  $S$  и массивы их элементов, которые распределяются по соответствующим подмассивам в массиве  $sub$ .

*Шаг 6.* Для каждой подалгебры из массива  $sub$  находятся все подалгебры покрывающие данную. Если в подмассиве  $sub[i+1]$  не нашлось ни одной подалгебры покрывающей данную, то ищем покрывающие из подмассива  $sub[i+2]$  и так далее. В результате получаем массив  $pokr$ , в котором записаны отношения покрытия для всех подалгебр алгебры  $S$ .

Данный алгоритм реализуется с помощью следующей программы.

#### **Программа нахождения отношения покрытия.**

```
pokr:=function(a,b,c,d)
    local A, El, i, j, k, y, sub, tip, S, s, s1, el, l, l1,
m, m1, n, n1, i1;
    sub:=[];
```

```

for i1 in [1..6] do
sub[i1]:=[];
                                od;

pokr:=[];
A:=MatAlgebra(GF(2),3);
El:=Elements(A);
S:=Subalgebra(A,[El[a],El[b],El[c],El[d]]);
    for i in S do
        for k in S do
            for j in S do
s1:=Subalgebra(S,[i,k,j]);
if Size(s1)=1 then
AddSet(sub[1],Elements(s1));fi;
if Size(s1)=2 then
AddSet(sub[2],Elements(s1));fi;
if Size(s1)=4 then
AddSet(sub[3],Elements(s1));fi;
if Size(s1)=8 then
AddSet(sub[4],Elements(s1));fi;
if Size(s1)=16 then
AddSet(sub[5],Elements(s1));fi;
                                od;
                            od;
                        od;
for m1 in [1..Size(sub)] do
    for l1 in [1..Size(sub[m1])] do
        for n1 in [1..Size(sub[m1+1])] do
if IsSubset(sub[m1+1][n1],sub[m1][l1])=true
then Add(pokr,[[m1,l1],[m1+1,n1]]);
fi;
                                od;
                            od;
                        od;
PrintTo("pokr.dan", pokr,"\n");

```

```
end;;
```

Далее запускается программа и прописывается команда `prokr(a,b,c,d)`, после выполнения которой, в файл *prokr.dan* записываются все отношения покрытия. Пример полученного результата.

```
[[[1,1],[2,1]], [[1,1],[2,2]], [[1,1],[2,3]], [[1,1],[2,4]],  
[[1,1],[2,5]], [[1,1],[2,6]], [[1,1],[2,7]], [[1,1],[2,8]],  
[[1,1],[2,9]], [[1,1],[2,10]], [[1,1],[2,11]], [[1,1],[2,12]],  
[[2,1],[3,1]], [[2,1],[3,2]], [[2,1],[3,3]], [[2,1],[3,4]],  
[[2,2],[3,1]], [[2,2],[3,5]], [[2,2],[3,6]], [[2,2],[3,7]],  
[[2,2],[3,8]], [[2,2],[3,9]], [[2,2],[3,10]], [[2,3],[3,1]],  
[[2,3],[3,11]], [[2,3],[3,12]], [[2,3],[3,13]], [[2,4],[3,2]],  
[[2,4],[3,5]], [[2,4],[3,11]], [[2,4],[3,14]], [[2,4],[3,15]],  
[[2,4],[3,16]], [[2,5],[3,2]], [[2,5],[3,6]], [[2,5],[3,17]],  
[[2,6],[3,6]], [[2,6],[3,11]], [[2,6],[3,18]], [[2,7],[3,3]],  
[[2,7],[3,7]], [[2,7],[3,14]], [[2,7],[3,17]], [[2,8],[3,3]],  
[[2,8],[3,8]], [[2,8],[3,12]], [[2,8],[3,15]], [[2,9],[3,7]],  
[[2,9],[3,12]], [[2,9],[3,16]], [[2,9],[3,18]], [[2,10],[3,4]],  
[[2,10],[3,9]], [[2,10],[3,14]], [[2,11],[3,4]], [[2,11],[3,10]],  
[[2,11],[3,13]], [[2,11],[3,15]], [[2,11],[3,17]], [[2,11],[3,18]], [[  
2,12],[3,9]], [[2,12],[3,13]], [[2,12],[3,16]], [[3,1],[4,1]],  
[[3,1],[4,2]], [[3,1],[4,3]], [[3,2],[4,1]], [[3,2],[4,4]],  
[[3,3],[4,2]], [[3,3],[4,4]], [[3,4],[4,3]], [[3,4],[4,4]],  
[[3,5],[4,1]], [[3,5],[4,5]], [[3,5],[4,6]], [[3,6],[4,1]],  
[[3,6],[4,7]], [[3,7],[4,2]], [[3,7],[4,5]], [[3,7],[4,7]],  
[[3,8],[4,2]], [[3,8],[4,6]], [[3,9],[4,3]], [[3,9],[4,5]],  
[[3,10],[4,3]], [[3,10],[4,6]], [[3,10],[4,7]], [[3,11],[4,1]],  
[[3,11],[4,8]], [[3,12],[4,2]], [[3,12],[4,8]], [[3,13],[4,3]],  
[[3,13],[4,8]], [[3,14],[4,4]], [[3,14],[4,5]], [[3,15],[4,4]],  
[[3,15],[4,6]], [[3,15],[4,8]], [[3,16],[4,5]], [[3,16],[4,8]],  
[[3,17],[4,4]], [[3,17],[4,7]], [[3,18],[4,7]], [[3,18],[4,8]],  
[[4,1],[5,1]], [[4,2],[5,1]], [[4,3],[5,1]], [[4,4],[5,1]],  
[[4,5],[5,1]], [[4,6],[5,1]], [[4,7],[5,1]], [[4,8],[5,1]]]
```

Пара  $[[1, 1], [2, 1]]$  означает что элемент  $[2, 1]$  покрывает  $[1, 1]$ , следовательно, элемент  $[2, 1]$  находится выше и данные элементы соединяются прямой.

По данному алгоритму были построены решетки для каждой таблицы умножения и классифицированы по типам решеток. Результаты построений:

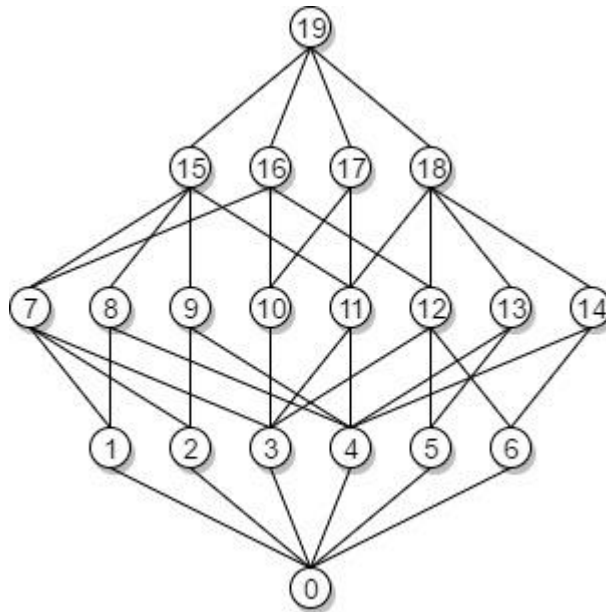


Рис.1. Тип решетки (1,6,8,4,1) Таблица 5

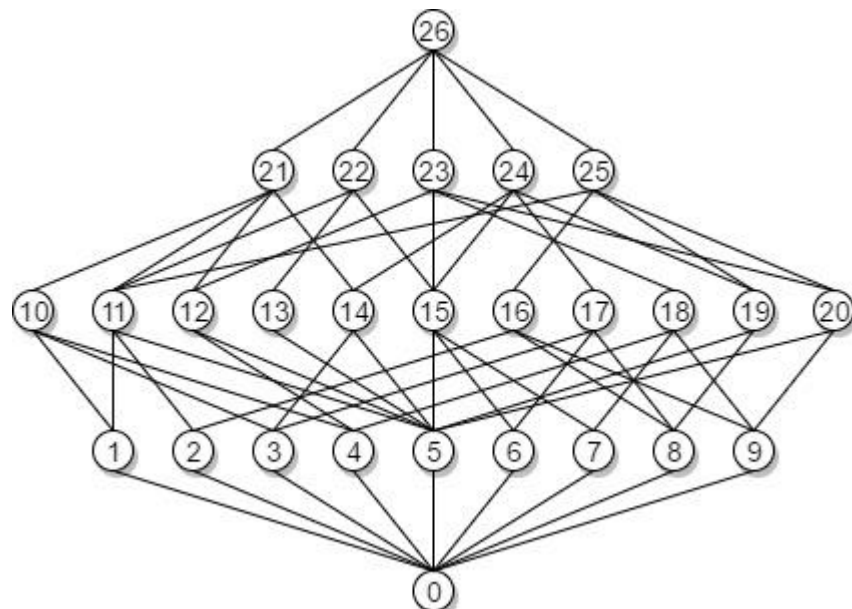


Рис.2. Тип решетки (1,9,11,5,1) Таблица 6

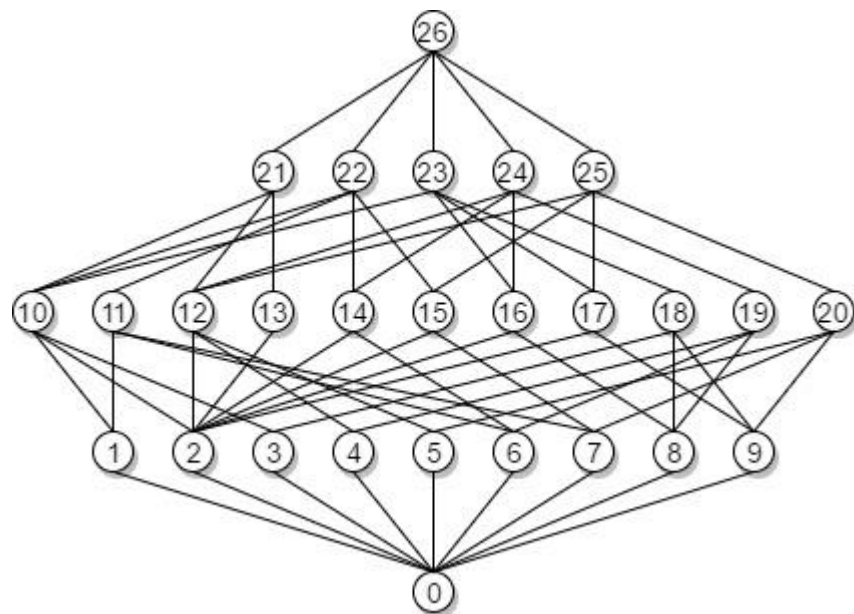


Рис.3. Тип решетки (1,9,11,5,1) Таблица 7

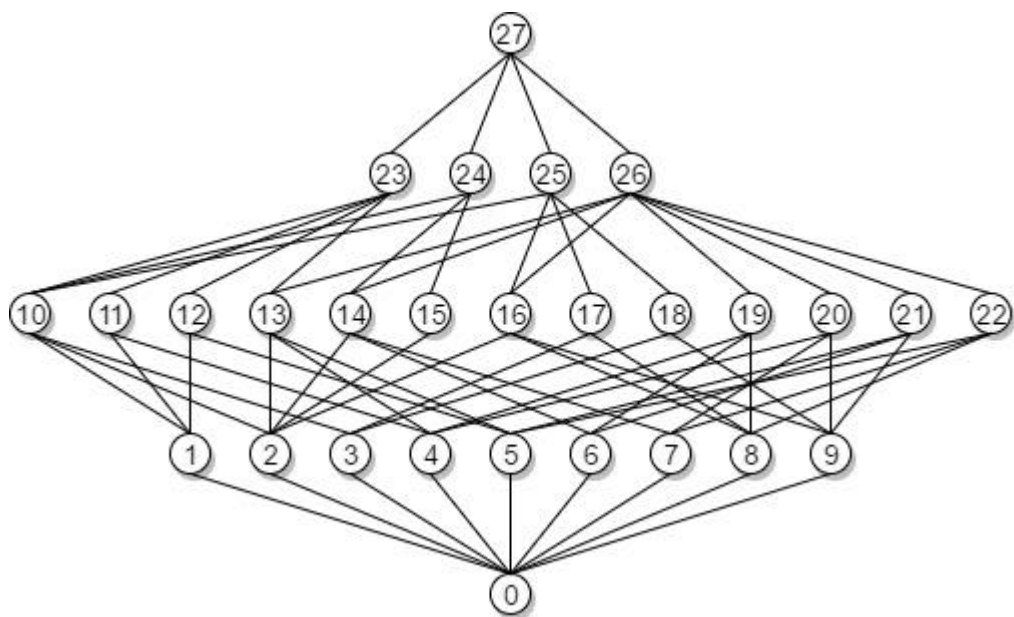


Рис.4. Тип решетки (1,9,13,4,1) Таблица 8

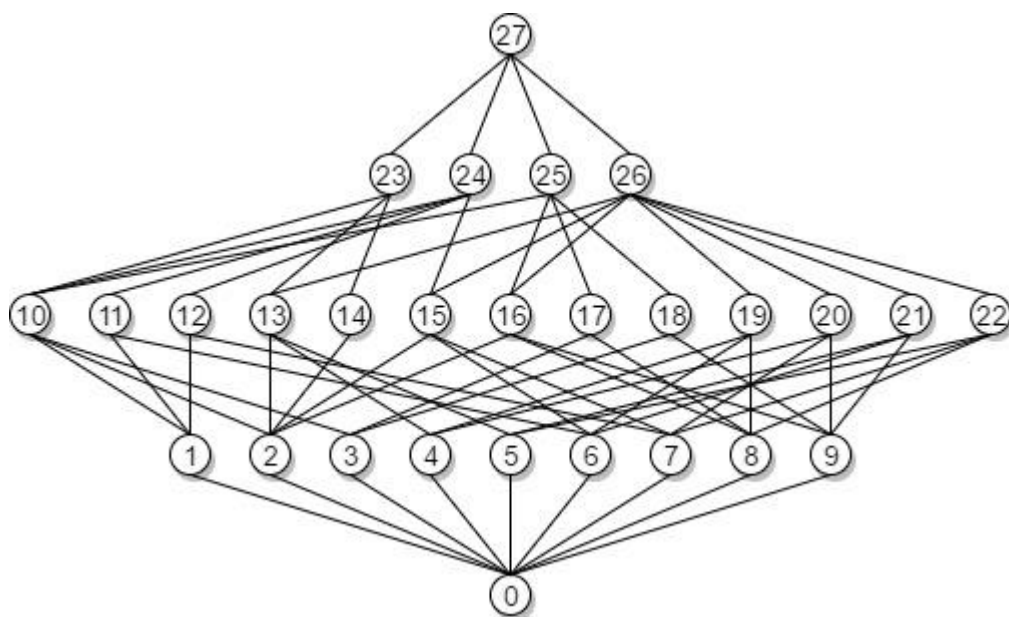


Рис.5. Тип решетки (1,9,13,4,1) Таблица 9

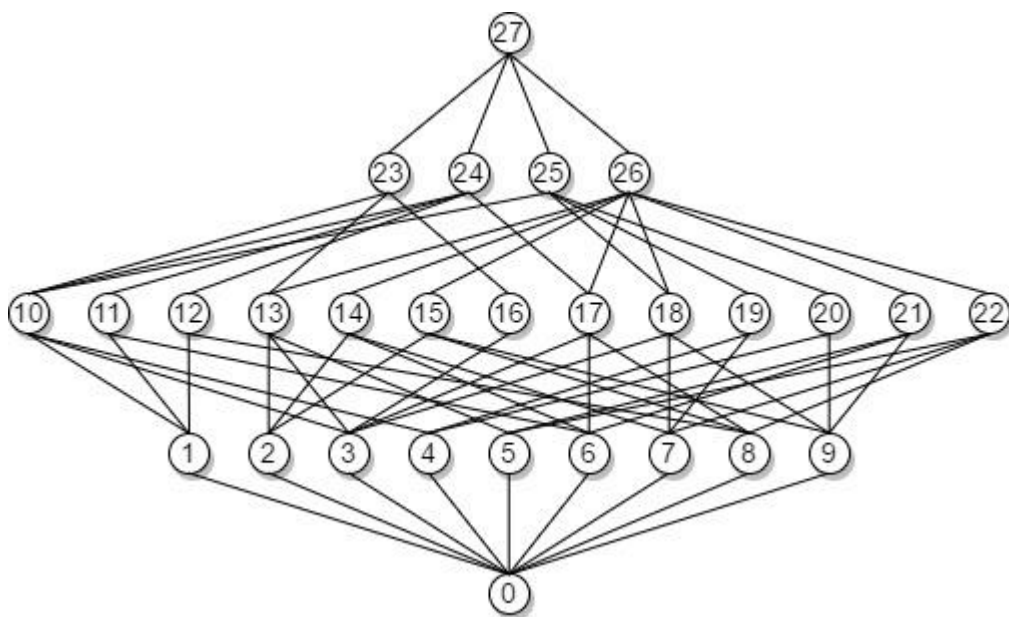


Рис.6. Тип решетки (1,9,13,4,1) Таблица 10



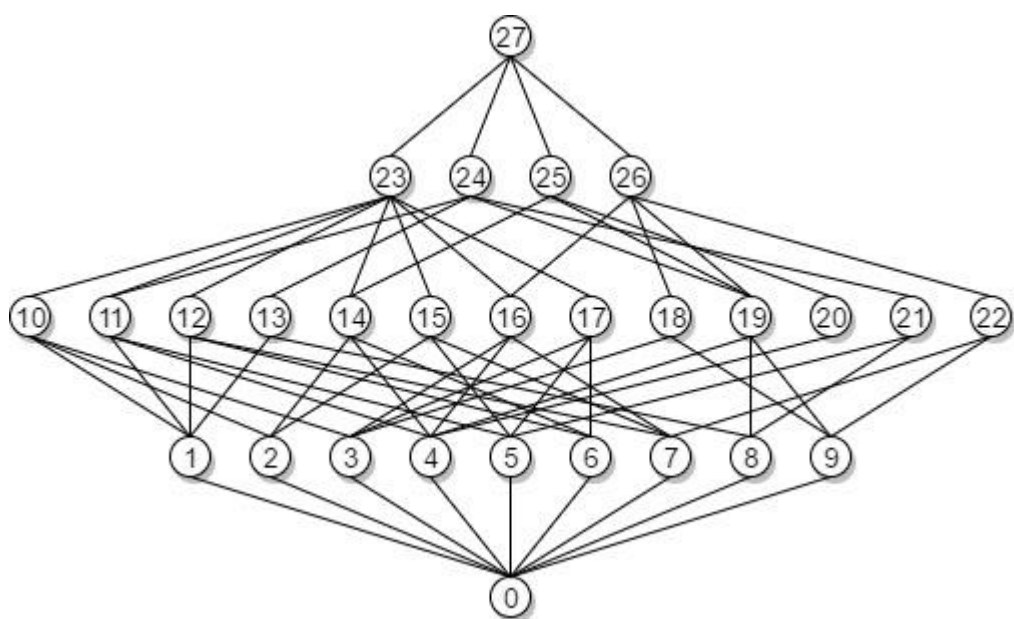


Рис.7. Тип решетки (1,9,13,4,1) Таблица 11

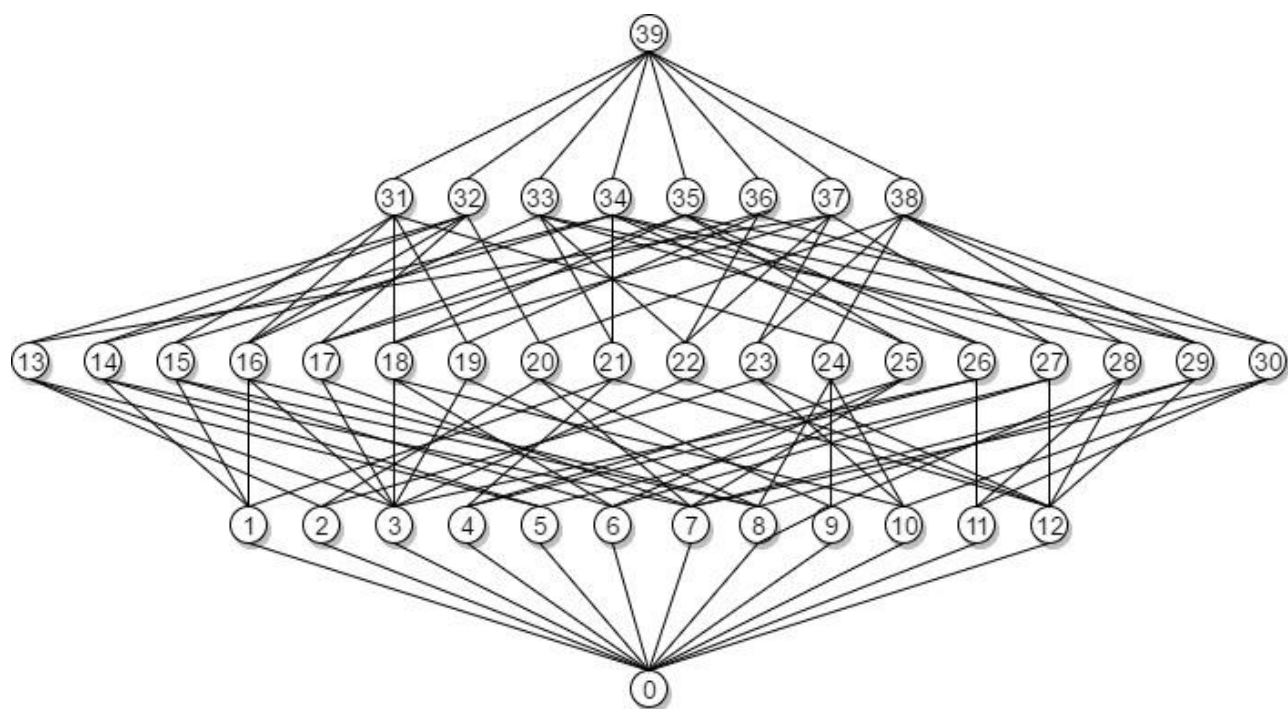


Рис.8. Тип решетки (1,12,18,8,1) Таблица 12

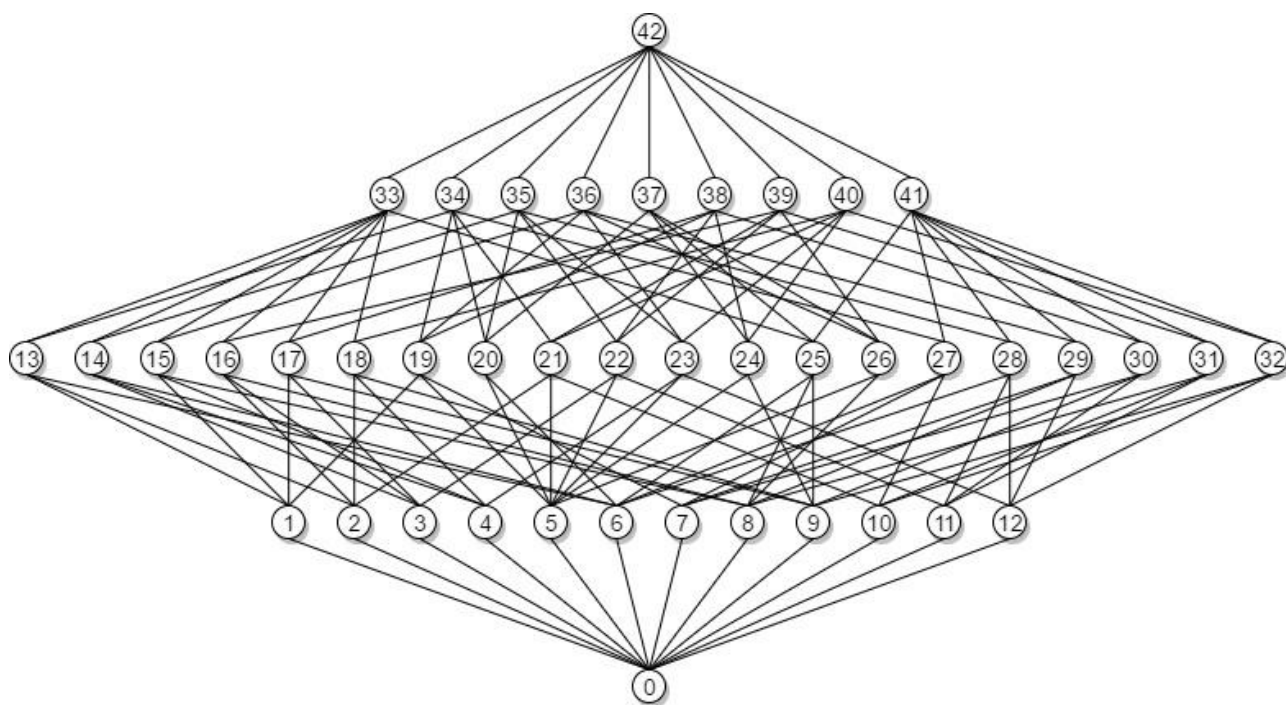


Рис.9. Тип решетки (1,12,20,9,1) Таблица 13

После построений возник вопрос об изоморфизме решеток, так как были получены решетки одного типа.

**Определение 29.** Биективное отображение  $\varphi$  решётки  $L$  в решётку  $L'$  называется решеточным изоморфизмом, если

$$(\forall x, y \in L)(\varphi(x \cup y) = \varphi(x) \cup \varphi(y)) \wedge (\varphi(x \cap y) = \varphi(x) \cap \varphi(y))$$

В результате проверки на изоморфизм, было обнаружено, что диаграммы решеток на Рис.2 и Рис.3, Рис.4 и Рис.5, Рис.6 и Рис.7 изоморфны между собой.

**Вывод:** неизоморфные алгебры с одним типом решетки могут иметь изоморфные решетки.

Таблица 14. Тип, диаграмма решетки и соответствующая таблица умножения

№	Порождающие элементы	Определяющая соответствие таблица умножения	Количество подалгебр	Тип решетки подалгебр	Диаграмма решетки																
1	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td><math>r_1</math></td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td><math>r_2</math></td></tr><tr><td><math>e</math></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	$r_1$	$r_2$	0	0	$r_2$	$e$	$r_1$	$r_2$	$e$	21	(1,6,8,4,1)	Рис.1
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	$r_1$																		
$r_2$	0	0	$r_2$																		
$e$	$r_1$	$r_2$	$e$																		

2	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td><math>r_1 + r_2</math></td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>e</math></td><td><math>r_2</math></td><td><math>r_2</math></td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$	$r_2$	0	0	0	$e$	$r_2$	$r_2$	$e$	21	(1,9,11,5,1)	Рис.2, Рис.3
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$																		
$r_2$	0	0	0																		
$e$	$r_2$	$r_2$	$e$																		
3	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td><math>r_2</math></td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td><math>r_2</math></td></tr><tr><td><math>e</math></td><td><math>r_1 + r_2</math></td><td>0</td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	$r_2$	$r_2$	0	0	$r_2$	$e$	$r_1 + r_2$	0	$e$	21	(1,9,11,5,1)	Рис.2, Рис.3
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	$r_2$																		
$r_2$	0	0	$r_2$																		
$e$	$r_1 + r_2$	0	$e$																		
4	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td><math>r_1 + r_2</math></td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>e</math></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$	$r_2$	0	0	0	$e$	$r_1$	$r_2$	$e$	21	(1,9,13,4,1)	Рис.4, Рис.5
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	$r_1 + r_2$																		
$r_2$	0	0	0																		
$e$	$r_1$	$r_2$	$e$																		
5	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td>0</td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>e</math></td><td><math>r_2</math></td><td><math>r_2</math></td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	0	$r_2$	0	0	0	$e$	$r_2$	$r_2$	$e$	21	(1,9,13,4,1)	Рис.4, Рис.5
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	0																		
$r_2$	0	0	0																		
$e$	$r_2$	$r_2$	$e$																		
6	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td><math>r_1</math></td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td><math>r_2</math></td></tr><tr><td><math>e</math></td><td><math>r_2</math></td><td><math>r_2</math></td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	$r_1$	$r_2$	0	0	$r_2$	$e$	$r_2$	$r_2$	$e$	21	(1,9,13,4,1)	Рис.6, Рис.7
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	$r_1$																		
$r_2$	0	0	$r_2$																		
$e$	$r_2$	$r_2$	$e$																		
7	$r_1, r_2, e$	<table><tr><td></td><td><math>r_1</math></td><td><math>r_2</math></td><td><math>e</math></td></tr><tr><td><math>r_1</math></td><td><math>r_1^2</math></td><td><math>r_1^2</math></td><td>0</td></tr><tr><td><math>r_2</math></td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>e</math></td><td><math>r_1 + r_2</math></td><td>0</td><td><math>e</math></td></tr></table>		$r_1$	$r_2$	$e$	$r_1$	$r_1^2$	$r_1^2$	0	$r_2$	0	0	0	$e$	$r_1 + r_2$	0	$e$	21	(1,9,13,4,1)	Рис.6, Рис.7
	$r_1$	$r_2$	$e$																		
$r_1$	$r_1^2$	$r_1^2$	0																		
$r_2$	0	0	0																		
$e$	$r_1 + r_2$	0	$e$																		

8	$r_1, e_1, e_2, e_3$	<table><tr><td></td><td><math>e_1</math></td><td><math>e_2</math></td><td><math>e_3</math></td><td><math>r_1</math></td></tr><tr><td><math>e_1</math></td><td><math>e</math></td><td>0</td><td>0</td><td><math>r_1</math></td></tr><tr><td><math>e_2</math></td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>e_3</math></td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td><math>r_1</math></td><td>0</td><td>0</td><td><math>r_1</math></td><td>0</td></tr></table>		$e_1$	$e_2$	$e_3$	$r_1$	$e_1$	$e$	0	0	$r_1$	$e_2$	0	0	0	0	$e_3$	0	0	0	0	$r_1$	0	0	$r_1$	0	84	(1,12,18,8,1)	Рис.8
	$e_1$	$e_2$	$e_3$	$r_1$																										
$e_1$	$e$	0	0	$r_1$																										
$e_2$	0	0	0	0																										
$e_3$	0	0	0	0																										
$r_1$	0	0	$r_1$	0																										
9	$r_1, r_2, e_1, e_2$	<table><tr><td></td><td><math>e_1</math></td><td><math>e_2</math></td><td><math>r_1</math></td><td><math>r_2</math></td></tr><tr><td><math>e_1</math></td><td><math>e_1</math></td><td>0</td><td><math>r_1</math></td><td><math>r_2</math></td></tr><tr><td><math>e_2</math></td><td>0</td><td><math>e_2</math></td><td>0</td><td>0</td></tr><tr><td><math>r_1</math></td><td>0</td><td><math>r_1</math></td><td>0</td><td>0</td></tr><tr><td><math>r_2</math></td><td>0</td><td><math>r_2</math></td><td>0</td><td>0</td></tr></table>		$e_1$	$e_2$	$r_1$	$r_2$	$e_1$	$e_1$	0	$r_1$	$r_2$	$e_2$	0	$e_2$	0	0	$r_1$	0	$r_1$	0	0	$r_2$	0	$r_2$	0	0	14	(1,12,20,9,1)	Рис.9
	$e_1$	$e_2$	$r_1$	$r_2$																										
$e_1$	$e_1$	0	$r_1$	$r_2$																										
$e_2$	0	$e_2$	0	0																										
$r_1$	0	$r_1$	0	0																										
$r_2$	0	$r_2$	0	0																										

## Библиографический список

1. Биркгоф Г., Теория решеток; пер. с англ. Салий В. Н. под ред. Скорнякова Л. А. – М.: Наука, 1984. – 568 с.
2. Гретцер Г. Общая теория решеток; пер. с англ. Больбота А. Д., Горбунова В. А., Туманова В. И. под ред. Смирнова Д. М. – М.: Мир, 1982. – 456 с.
3. Калужнин Л. А. Введение в общую алгебру. – М.: Наука, 1973. – 448 с.
4. Коробков С. С. Введение в теорию решеток: Учеб. пособие по спец. курсу. Урал. гос. пед. ун-т. — Екатеринбург: Б.и., 1996. – 64с.
5. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец. "Математика", "Приклад. математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432с.
6. Курош А. Г. Лекции по общей алгебре: учебник. – СПб.: Лань, 2005. – 560 с.
7. Гришина А.А. Подалгебры матричной алгебры  $M_3(GF(2))$ . Дипломная работа. УрГПУ. Екатеринбург. 2003.
8. Васильев С.А. Использование прикладного пакета GAP для описания решеток подалгебр моногенных трехмерных алгебр над полем  $GF(2)$ . Дипломная работа. УрГПУ. Екатеринбург. 2016.
9. Бочарова Т.С. Использование прикладного пакета GAP для описания решеток подалгебр трехмерных алгебр над полем  $GF(2)$ . Дипломная работа. УрГПУ. Екатеринбург. 2016.
10. Система компьютерной алгебры GAP – Exponenta. Режим доступа: [www.exponenta.ru/soft/others/gap/1.asp](http://www.exponenta.ru/soft/others/gap/1.asp)
11. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>

# Приложения

## Массив матриц алгебры $A = M_3(GF(2))$

[illegible]









58

59







53